

Resolver problemas los entornos del Switching de LAN

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Convenciones](#)

[Introducción a LAN Switching](#)

[Hubs y switches](#)

[Puentes y switches](#)

[VLAN](#)

[Algoritmo de puente transparente](#)

[Spanning Tree Protocol](#)

[Trunking](#)

[EtherChannel](#)

[Conmutación de Capas Múltiple \(MLS\)](#)

[Cómo obtener más información sobre estas características](#)

[Sugerencias para la solución de problemas de router generales](#)

[Troubleshooting de Conectividad de Puerto](#)

[Problemas del hardware](#)

[Problemas de configuración](#)

[Problemas de tráfico](#)

[Falla de hardware del switch](#)

[Resolución de problemas de negociación automática half/full duplex de Ethernet 10/100/ Mb](#)

[Objetivos](#)

[Introducción](#)

[Resolución de la negociación automática de Ethernet entre los dispositivos de infraestructura de la red](#)

[Procedimientos y/o escenarios](#)

[Ejemplo de configuración y resolución de problemas de negociación automática de Ethernet de 10/100 Mb.](#)

[Paso a paso](#)

[Antes de que usted llame al equipo de Soporte técnico de Cisco Systems](#)

[Configuración de las conexiones switch-a-switch EtherChannel de los switches Catalyst 4000/5000/6000](#)

[Tareas para la configuración manual del EtherChannel](#)

[Paso a paso](#)

[Verifique la Configuración](#)

[Utilice el PAgP para configurar el EtherChannel \(el método preferido\)](#)

[Enlace troncal y EtherChannel](#)

[Resolución de problemas de EtherChannel](#)

[Comandos utilizados en esta sección](#)

[Utilización de Portfast y otros comandos para solucionar los problemas al iniciar la conectividad de la estación extremo](#)

[Contenido](#)

[Antecedente](#)

[Cómo reducir el retardo de inicialización en el switch Catalyst 4000/5000/6000](#)

[Pruebas de sincronización con y sin DTP, PagP y PortFast en Catalyst 5000](#)

[Cómo reducir el retardo de inicialización en el switch Catalyst 2900XL/3500XL](#)

[Pruebas de Timing en el Catalyst 2900XL](#)

[Cómo reducir el retardo de inicialización en el switch Catalyst 1900/2800](#)

[Pruebas de sincronización en el Catalyst 1900](#)

[Beneficio adicional de Portfast](#)

[Los comandos de utilizar para verificar la configuración trabajan](#)

[Comandos de utilizar para resolver problemas la configuración](#)

[Multi-Layer Switching \(MLS\) IP de la configuración y del Troubleshooting](#)

[Objetivos](#)

[Introducción](#)

[Resolución de problemas de la tecnología IP MLS](#)

[Comandos o capturas de pantalla](#)

[Antes de que usted llame el equipo de Soporte técnico de Cisco Systems](#)

[Información Relacionada](#)

Introducción

Las secciones en este capítulo describen las funciones del LAN Switch y las soluciones a algunos problemas de LAN Switching más comunes. Se cubren estos elementos:

- Introducción a LAN Switching
- Sugerencias para la solución de problemas de router generales
- Troubleshooting de Conectividad de Puerto
- Resolución de problemas de negociación automática half/full duplex de Ethernet 10/100/ Mb
- Trunking ISL en switches de la familia Catalyst 5000 y 6000
- Configuración y solución de problemas de EtherChannel switch a switch
- Usando Portfast y otros comandos de reparar los problemas de conectividad del inicio de estación extrema
- Configuración y resolución de problemas relacionados con la conmutación de capas múltiples

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Introducción a LAN Switching

Si usted es nuevo al Switching de LAN, estas secciones le toman con algunos de los conceptos principales relacionados con el Switches. Uno de los requisitos previos para la resolución de problemas de cualquier dispositivo es conocer las reglas bajo las que trabaja. El Switches ha llegado a ser mucho más complejo en los últimos años porque él ha ganado en el renombre y la sofisticación. Estos párrafos describen algunos de los conceptos fundamentales para saber sobre el Switches.

Hubs y switches

Debido a la gran demanda puesta en las redes de área local, hemos visto una rotación de una red del ancho de banda compartido, con el Hubs y el cable coaxial, a una red del Ancho de banda dedicado, con el Switches. Un concentrador permite que varios dispositivos se conecten al mismo segmento de red. Los dispositivos en ese segmento comparten el ancho de banda con uno a. Si es un concentrador 10Mb, y hay 6 dispositivos conectados con 6 diversos puertos en el concentrador, los seis dispositivos comparten el 10Mb del ancho de banda con uno a. Un concentrador 100Mb comparte 100Mb del ancho de banda entre los dispositivos conectados. En términos de modelo de OSI, un concentrador se considera un dispositivo de la capa-uno (Capa física). Escucha una señal eléctrica en el cable y la transfiere por los otros puertos.

Un Switch puede substituir físicamente un concentrador en su red. Un Switch permite que los dispositivos múltiples sean conectados con la misma red, apenas como lo hace un concentrador, pero aquí es donde la semejanza termina. Un Switch permite que cada dispositivo conectado tenga Ancho de banda dedicado en vez del ancho de banda compartido. El ancho de banda entre el switch y el dispositivo está reservado para la comunicación hacia y desde ese dispositivo en forma exclusiva. Seis dispositivos conectaron con seis diversos puertos en un 10Mb Switch que cada uno tiene 10Mb del ancho de banda a trabajar con, en vez del ancho de banda compartido con los otros dispositivos. Un switch puede incrementar en gran medida el ancho de banda disponible de su red, lo cual puede conducir a una mejora en el rendimiento de la red.

Puentes y switches

Un Switch básico se considera un dispositivo de la capa-dos. Cuando usamos la palabra capa, nos referimos al modelo OSI de 7 capas. Un Switch apenas no pasa las señales eléctricas adelante, como un concentrador hace; en lugar, ensambla las señales en una trama (capa dos), y después decide qué hacer con la trama. Un Switch determina qué hacer con una trama pidiendo prestado un algoritmo de otro dispositivo de interconexión de redes común: un Bridge transparente. Lógicamente, un switch actúa como lo haría un puente transparente, pero puede administrar tramas mucho más rápidamente que un puente transparente (debido al hardware y arquitectura especiales). Una vez que un switch decide adónde se debe enviar la trama, la pasa a través de los puertos apropiados. Piense en un switch como un dispositivo que crea conexiones instantáneas entre varios puertos de trama en trama.

VLAN

Puesto que el Switch decide sobre una trama por la base de la trama que vira los intercambiables

datos hacia el lado de babor, es una extensión natural para poner la lógica dentro del Switch para permitir que elija los puertos para las agrupaciones especiales. A este agrupamiento de puertos se lo denomina Red virtual de área local (VLAN). El switch se asegura que el tráfico de un grupo de puertos nunca se envíe a otros grupos de puertos (los que serán ruteos). Estos grupos de puertos (VLAN) se pueden cada uno considerar un segmento LAN individual.

Los VLAN también se describen como dominios de broadcast. El está debido al Transparent Bridging Algorithm, que dice que los paquetes de broadcast (paquetes destinados para *todo el direccionamiento de dispositivos*) estén enviados todos los puertos que estén en el mismo grupo (es decir, en el mismo VLAN). Todos los puertos que están en el mismo VLAN están también en el mismo dominio de broadcast.

Algoritmo de puente transparente

El Transparent Bridging Algorithm y el *atravesar - el árbol* se cubre más detalladamente a otra parte (el capítulo 20: Resolviendo problemas los entornos de Transparent Bridging). Al recibir una trama, el switch debe decidir qué hará con ella. Podría ignorar la trama; podría pasar la trama hacia fuera otro puerto, o podría pasar la trama hacia fuera muchos otros puertos.

Para conocer qué hacer con la trama, el Switch aprende la ubicación de todos los dispositivos en el segmento. Esta información sobre la ubicación se pone en una tabla del Content Addressable Memory (CAM - nombrado para el tipo de memoria usado para salvar estas tablas). La tabla CAM muestra, para cada dispositivo, la dirección MAC del dispositivo, hacia fuera cuál puerto que la dirección MAC puede ser encontrada, y con qué VLAN es asociado este puerto. El Switch hace continuamente este proceso de aprendizaje mientras que las tramas se reciben en el Switch. La tabla CAM del Switch es continuamente actualizada.

Esta información en la tabla CAM se utiliza para decidir a cómo se maneja una trama recibida. Para decidir a donde enviar una trama, las miradas del Switch en la dirección MAC del destino en una trama recibida y miran para arriba esa dirección MAC del destino en la tabla CAM. Las demostraciones de la tabla CAM que viran la trama hacia el lado de babor se deben enviar para que esa trama alcance la dirección MAC del destino especificado. Aquí están las reglas básicas que un Switch utiliza para realizar la responsabilidad del reenvío de tramas:

- Si la dirección MAC del destino se encuentra en la tabla CAM, el Switch manda la trama el puerto que se asocia a esa dirección MAC del destino en la tabla CAM. Está llamada se está desviando.
- Si el puerto asociado para enviar la trama hacia fuera es el mismo puerto que vino la trama originalmente adentro encendido, no hay necesidad de enviar la trama se retira ese mismo puerto, y se ignora la trama. Este proceso se denomina filtrado.
- Si la dirección MAC del destino no está en la tabla CAM (el direccionamiento es *desconocido*), el Switch manda la trama el resto de los puertos que estén en el mismo VLAN que la trama recibida. Esto se denomina inundación. No inunda la trama hacia fuera el mismo puerto en el cual la trama fue recibida.
- Si la dirección MAC del destino de la trama recibida es la dirección de broadcast (FFFF.FFFF.FFFF), la trama se envía todos los puertos que estén en el mismo VLAN que la trama recibida. Esto también se llama inundación. La trama no se envía el mismo puerto en el cual la trama fue recibida.

Spanning Tree Protocol

Como hemos visto, el algoritmo de conexión en puente transparente emite tramas desconocidas y de transmisión a través de todos los puertos que están en la misma VLAN que la trama recibida. Esto causa un posible problema. Si los dispositivos de red que funcionan con este algoritmo están conectados juntos en un loop físico, las tramas inundadas (como los broadcasts) se pasan del Switch para conmutar, alrededor y alrededor del loop, para siempre. El dependiente sobre las conexiones físicas implicadas, las tramas puede multiplicar realmente exponencial debido al algoritmo de inundación, que puede causar los problemas de red grave.

Hay una ventaja a un loop físico en su red: puede proporcionar la Redundancia. Si un link falla, aún existe otra forma e que el tráfico llegue a su destino. Para permitir las ventajas derivadas de la Redundancia, sin la fractura de la red debido a la inundación, un protocolo llamado el atravesar - el árbol fue creado. El árbol de expansión fue estandarizado en la especificación IEEE 802.1d.

El propósito del Spanning Tree Protocol (STP) es identificar y bloquear temporalmente los loops en un segmento de red o un VLAN. Los switches ejecutan el STP, lo que implica la elección de un puente de la raíz o switch. Los otros switches miden su distancia desde el switch raíz. Si hay más de una manera de conseguir al switch de la raíz, hay un loop. El Switches sigue el algoritmo para determinar qué puertos se deben bloquear para romper el loop. El STP es dinámico; si un link en el segmento falla, los puertos que bloqueaban originalmente se pueden cambiar posiblemente al modo de reenvío.

Trunking

El enlace troncal es un mecanismo que generalmente se utiliza para permitir que varias VLAN funcionen independientemente a través de varios switches. El Routers y los servidores pueden utilizar el enlace, también, que permite que vivan simultáneamente en los VLAN múltiples. Si su red tiene solamente un VLAN en ella, usted puede ser que nunca necesite el enlace; pero si su red tiene más de un VLAN, usted quiere probablemente aprovecharse de las ventajas del enlace.

Un puerto en un Switch pertenece normalmente a solamente un VLAN; cualquier tráfico recibido o enviado encendido este puerto se asume para pertenecer al VLAN configurado. Por otra parte, un puerto troncal es un puerto que puede ser configurado para enviar y recibir tráfico para varias VLAN. Logra esto cuando adjunta la información de VLAN a cada trama, un proceso llamado *marcar la trama con etiqueta*. También, el enlace debe ser activo a ambos lados del link; el otro lado debe contar con las tramas que incluyen la información de VLAN para que ocurra la comunicación correcta.

Hay métodos distintos de dependiente del enlace sobre el media se utiliza que. Los métodos de concentración de link troncal para Fast Ethernet o Gigabit Ethernet son el link entre switches (ISL) o 802.1q. El enlace troncal sobre ATM usa LANE. Enlace sobre las aplicaciones 802.10 FDDI.

EtherChannel

El EtherChannel es una técnica se utiliza que cuando usted tiene conexiones múltiples al mismo dispositivo. Bastante que cada función del link independientemente, grupos EtherChannel los puertos junto a trabajar como una unidad. Distribuye el tráfico a través de todos los links y proporciona la Redundancia si uno o más links fallan. Las configuraciones EtherChannel tienen que ser iguales en ambos lados de los links que forman parte del canal. Normalmente, atravesando - el árbol bloquearía todas estas conexiones paralelas entre los dispositivos porque son loops, pero el EtherChannel se ejecuta *por debajo* atravesar - el árbol, de modo que atravesando - el árbol piensa que todos los puertos dentro de un EtherChannel dado son solamente un puerto único.

Conmutación de Capas Múltiple (MLS)

El Multilayer Switching (MLS) es la capacidad de un Switch de remitir las tramas basadas en la información en el capa tres y a veces la encabezado de la capa-cuatro. Esto se aplica a los paquetes del IP pero ahora también puede generalmente ocurrir para los paquetes IPX. El Switch aprende cómo manejar estos paquetes cuando comunica con los routers o más. Con una explicación simplificada, los relojes del Switch cómo los procesos del router un paquete, y entonces el Switch procesa los paquetes futuros en este mismo flujo. Tradicionalmente, los switches eran mucho más rápidos en las tramas de conmutación que los routers, por lo que hacerlos descargar el tráfico proveniente del router puede resultar en importantes mejoras de velocidad. Si algo cambia en la red, el router puede decir el Switch borrar su caché del capa tres y construirlo desde el principio otra vez mientras que la situación se desarrolla. El protocolo utilizado para comunicarse con los routers se denomina Protocolo de conmutación de capas múltiples (MLSP).

Cómo obtener más información sobre estas características

Éstas son sólo algunas de las características básicas que admiten los switches. Más se agregan cada día. Es importante entender cómo su Switches funciona, que le ofrece uso, y cómo esas características debe trabajar. Uno de los mejores lugares para aprender esta información sobre los switches Cisco está en el sitio Web de Cisco. Vaya y bajo al *servicio y a soporte de la* sección, eligen los *documentos técnicos*. De aquí, elija el *Home Page de la documentación*. Los conjuntos de documentación para todos los Productos Cisco se pueden encontrar aquí. *Los switches LAN de múltiples capas* conectan los leads usted a la documentación para todos los switches LAN de Cisco. Para aprender sobre las características de un Switch, lea la *guía de configuración de software* para la versión particular de software que usted utiliza. Las guías de configuración de software le dan la información previa sobre lo que hace la característica y qué comandos de utilizar para configurarlo en su Switch. Toda esta información está disponible en forma gratuita en la Web. Usted ni siquiera necesita un explicar esta documentación; está disponible para cualquier persona. Algunas de estas guías de configuración se pueden leer adentro una tarde y están bien digno del tiempo pasado.

El sitio web del soporte y de la documentación de Cisco puebla a otra parte del sitio Web de Cisco. Se llena de la información diseñada para ayudarle a implementar, a mantener, y a resolver problemas su red. Vaya al sitio web del [soporte y de la documentación](#) a conseguir la información de servicio técnico detallada por los Productos o las Tecnologías específicos.

Sugerencias para la solución de problemas de router generales

Hay muchas maneras de resolver problemas un Switch. Mientras que las características del Switches crecen, las cosas posibles que pueden romperse también aumentan. Si usted desarrolla un acercamiento o un plan de prueba para resolver problemas, usted es mejor de a largo plazo que si usted apenas intenta un acercamiento de la golpe-y-falta. Aquí están algunas sugerencias generales para hacer su resolver problemas más eficaz:

- Tómese el tiempo para familiarizarse con el funcionamiento normal del switch. El sitio Web de Cisco tiene una cantidad enorme de información técnica que describa cómo su Switches funciona, como se menciona en la sección anterior. En especial las guías de configuración son muy útiles. Se abren muchos casos que se solucionan con la información de las guías de configuración del producto.

- Para las más situaciones complejas, tenga un físico preciso y un mapa lógico de su red. Una correspondencia física muestra cómo los dispositivos y los cables están conectados. Un mapa lógico muestra qué segmentos (VLAN) exista en su red y qué Routers proporciona los servicios de ruteo a estos segmentos. El atravesar - la correspondencia del árbol es altamente útil para resolver problemas los temas complejos. Debido a la capacidad de un Switch de crear diversos segmentos con la implementación de los VLAN, las conexiones físicas solamente no cuentan la historia completa; uno tiene que saber el Switches se configura para determinar que existen los segmentos (VLAN) y saber están conectados lógicamente.
- Tenga un plan. Algunos problemas y soluciones son obvios; algunos no son. Los síntomas que usted ve en su red pueden ser el resultado de los problemas en otra área o capa. Antes de que usted salte a las conclusiones, intente verificar de una manera estructurada qué trabaja y qué no lo hace. Puesto que las redes pueden ser complejas, es útil aislar los dominios del Posible problema. Una manera de hacer esto es utilizar el modelo de la siete-capas OSI. Por ejemplo: marque las conexiones físicas implicadas (la capa 1); marque los problemas de conectividad dentro del VLAN (la capa 2), y marca los problemas de conectividad a través de diversos VLAN (capa 3), etc. Si hay una configuración correcta en el Switch, muchos de los problemas que usted encuentra se relacionan con los problemas de la capa física (los puertos físicos y cableado). Hoy, el Switches está implicado en el capa tres y cuatro problemas, que la inteligencia incorporada de conmutar los paquetes basados en la información derivada del Routers, o realmente tiene el Routers que vivo dentro del Switch (capa tres o transferencia de la capa-cuatro).
- No asuma los trabajos de un componente sin marcarla primero. Esto puede ahorrarle mucho tiempo perdido. Por ejemplo, si un PC no puede iniciar sesión a un servidor a través de su red, hay muchas cosas que pueden ser incorrectas. No salte las cosas básicas y asuma que algo trabaja; alguien puede haber cambiado algo y no haber dichole. Tarda solamente un minuto para marcar algunas de las cosas básicas (por ejemplo, eso los puertos implicados está conectada con el lugar correcto y es activo), que podrían salvarle muchas horas perdidas.

Troubleshooting de Conectividad de Puerto

¡Si el puerto no trabaja, nada trabaja! Los puertos son la base de la red de conmutación. Algunos puertos tienen significado especial debido a su ubicación en la red y la cantidad de tráfico que llevan. Estos puertos incluyen las conexiones a otros Switches, Routers, y servidores. Puede ser más difícil resolver problemas en estos puertos porque, generalmente, aprovechan las funciones especiales como el enlace troncal y EtherChannel. El resto de los puertos es significativo, también, porque conectan a los usuarios reales de la red.

Muchas cosas pueden hacer un puerto ser no funcional: problemas del hardware, problemas de configuración, y problemas del tráfico. Estas categorías son un poco más profundas explorado.

'Problemas del hardware

General

La funcionalidad de puerto requiere dos puertos de funcionamiento conectados por un cable en funcionamiento (del tipo correcto). El valor por defecto de la mayoría de los switches Cisco es

tener un puerto en el *notconnectstate*, así que significa que no está conectado actualmente con cualquier cosa sino que quiere conectar. Si usted conecta un buen cable con dos puertos del switch en el *estado no conectado*, la luz de link llega a ser verde para ambos puertos, y el estado del puerto dice *conectado*, que significa que el puerto está para arriba por lo que la capa una. Estos párrafos señalan los elementos para que marquen si la capa una no está para arriba.

Revise el estado del puerto para ambos puertos involucrados. Asegúrense que ningún puerto que forme parte de este link esté cerrado. El administrador puede haber apagado posiblemente un o ambos puertos. El software dentro del Switch puede haber cerrado el puerto debido a las condiciones de error de configuración (nos ampliaremos en esto más adelante). Si es un lado apaga y el otro no es, el estatus en el lado habilitado es *notconnect* (porque no detecta a un vecino en el otro lado del alambre). El estatus en el lado de cierre normal dice algo como la *neutralización* o el *errdisable* (dependiente sobre qué cerró realmente el puerto). El link no sube a menos que se habiliten ambos puertos.

Cuando usted engancha encima de un buen cable (otra vez, si es del tipo correcto) entre dos puertos habilitados muestran una luz de link verde dentro de algunos segundos. También, las demostraciones del estado de puerto *conectadas* en el comando line interface(cli). En este momento, si usted no tiene link, su problema se limita a tres cosas: el puerto en un lado, el puerto en el otro lado, o el cable en el centro. En algunos casos, hay los otros dispositivos implicados: los conversores de medios (fibra a revestir con cobre, etc.), o en los links Gigabit usted puede tener conectores de interfaz Gigabit (GBIC). No obstante, esto es razonablemente una área limitada a buscar.

Los conversores de medios pueden agregar el ruido a una conexión o debilitar la señal si no funcionan correctamente. También agregan los conectores adicionales que pueden causar los problemas y son otro componente a hacer el debug de.

Verifique conexiones débiles. Un cable aparece a veces ser asentado en el conector, pero no está realmente; desenchufe el cable y reinsértelo. Usted debe también buscar la suciedad o los contactos rotos o perdidos. Realice esto para ambos puertos que forman parte de la conexión.

El cable se puede enchufar al puerto incorrecto, que sucede comúnmente. Asegúrese los ambos extremos del cable se enchufan a los puertos en donde usted los quiere realmente.

Se puede tener un link en uno de los lados y en el otro no. Ambos lados del control para el link. Un simple cable dañado puede provocar este tipo de problema.

Una luz de link no garantiza que el cable funcione correctamente. Puede haber encontrado la tensión física que la hace ser funcional en un nivel marginal. Usted nota generalmente esto por el puerto que tiene porciones de errores de paquete.

Para determinar si el cable es el problema, intercámbielo con un buen cable sabido. Apenas no lo intercambie con ningún otro cable; asegúrese que usted lo intercambia con un cable que usted conozca sea bueno y sea del tipo correcto.

Si esto es una extensión del cable muy larga (metro, a través de un campus grande, por ejemplo), es agradable tener un probador de cable complejo. Si usted no tiene un probador de cable, usted puede considerar éstos:

- Intente diversos puertos para ver si suben con este cable largo.
- Conecte el puerto en la pregunta con otro puerto en el mismo Switch apenas para ver si los links del puerto para arriba localmente.

- Vuelva a poner temporalmente el Switches cerca de uno a, así que usted puede probar un buen cable sabido.

Cobre

Asegurese que usted tiene el cable correcto para el tipo de conexión que usted hace. El cable de la categoría 3 se puede utilizar para las conexiones UTP 10MB, pero la categoría 5 se debe utilizar para 10/100 de las conexiones.

Un cable continuo RJ-45 se utiliza para que las estaciones finales, al Routers, o los servidores conecten con un Switch o un concentrador. Un cable de par cruzado de Ethernet se utiliza para el Switch para conmutar o el concentrador a las conexiones del switch. Éste es el pin-hacia fuera para un cable de par cruzado de Ethernet. Las distancias máximas para los cables de cobre de Ethernet o Fast Ethernet es de 100 metros. Una buena regla práctica general es que cuando usted cruza una capa OSI, como entre un Switch y un router, utiliza un cable de conexión directa; cuando usted conecta dos dispositivos en la misma capa OSI, como entre dos Routers o dos Switches, utilice una cruz sobre el cable. Con el objetivo de aplicar únicamente esta regla, trate a la estación de trabajo como un router.

Estos dos gráficos muestran las pin-salidas requeridas para un cable de par cruzado de switch a switch.

'Fibra'

Para la fibra, asegurese que usted tiene el cable correcto para las distancias implicadas y el tipo de puertos de fibra se utiliza que (modo simple, modo múltiple). Asegurese los puertos que están conectados juntos son modo simple o ambos puertos de modo múltiple. La fibra de modo único alcanza generalmente 10 kilómetros, y la fibra de modos múltiples puede alcanzar generalmente 2 kilómetros, pero hay el caso especial de con varios modos de funcionamiento 100BaseFX usado en el modo semidúplex, que puede ir solamente 400 contadores.

Para las conexiones de fibra, asegurese el lead del transmitir de un puerto está conectado con el lead de la recepción del otro puerto, y vice versa; transmita para transmitir, reciba para recibir, no trabaja.

Para conexión Gigabit, los GBIC deben coincidir en cada extremo de la conexión. Hay diversos tipos de GBIC dependientes sobre el cable y las distancias implicados: Longitud de onda corta (SX), longitud de onda larga/Trayecto largo (LX/LH), y distancia extendida (ZX).

Un SX GBIC necesita conectar con un SX GBIC; un SX GBIC no conecta a un LX GBIC. También, algunas conexiones Gigabit requieren los cables de acondicionamiento dependientes sobre las longitudes implicadas. Refiera a las notas de la instalación GBIC.

Si no sube su link Gigabit, marcar para asegurarse las configuraciones del control de flujo y de la negociación de puerto sea constante a ambos lados del link. Puede haber incompatibilidades en la implementación de estas características si el Switches que está conectado es de diversos vendedores. Si tiene dudas, apague estas funciones en ambos switches.

Problemas de configuración

Otra causa de los problemas de conectividad de puerto es la configuración de software incorrecta del switch. Si un puerto tiene una luz anaranjada no intermitente, esa significa que ese software dentro del Switch apaga el puerto, por la interfaz de usuario o por los procesos internos.

Asegúrese que el administrador no ha apagado los puertos implicados (según lo mencionado). El administrador puede haber apagado manualmente el puerto en un lado del link o el otro. Este link no sube hasta que usted vuelva a permitir el puerto; marque el estado del puerto.

Un poco de Switches, tal como el Catalyst 4000/5000/6000, puede apagar el puerto si los procesos del software dentro del Switch detectan un error. Cuando usted mira el estado del puerto, lee el *errdisable*. Debe arreglar el problema de configuración y luego sacar manualmente al puerto del estado *errDisable*. Algunas versiones de software más recientes (CatOS 5.4(1) y posterior) pueden volver a activar un puerto automáticamente después de un período de tiempo configurable transcurrido en el estado *errDisable*. Éstos son algunas de las causas para este estado de *errDisable*:

- **Error de configuración EtherChannel:** Si un lado se configura para el EtherChannel y no es el otro, puede causar atravesar - proceso del árbol para apagar el puerto en el lado configurado para el EtherChannel. Si usted intenta configurar el EtherChannel pero los puertos implicados no tienen las mismas configuraciones (velocidad, duplex, modo de concentración links, etc.) como sus puertos de vecino a través del link, podría causar al estado de *errDisable*. Es el mejor fijar cada lado para el *desirable mode* del EtherChannel si usted quiere utilizar el EtherChannel. Las secciones hablan después profundizado sobre cómo configurar el EtherChannel.
- **Discordancia dúplex:** Si el puerto del switch recibe un montón de colisiones tardías, esto indica generalmente un problema de incompatibilidad de dúplex. Hay otras causas para los lates colisiones: un mín NIC, los segmentos del cable que son demasiado largos, solamente la mayoría de las razones comunes es hoy una discordancia dúplex. El lado de dúplex completo piensa que puede enviar siempre que quiera a. El lado semidúplex cuenta con solamente los paquetes a veces - no en "cualquier" hora.
- **Puerto de protección BPDU:** Algunas versiones nuevas de software de switch pueden monitorear si portfast está habilitada en un puerto. Un puerto que utiliza el portfast se debe conectar con una estación final, no con los dispositivos que generan los paquetes del árbol de expansión llamados los BPDU. Si el Switch nota un BPDU que venga en un puerto que tenga portfast habilitado, pone el puerto en el modo *errDisable*.
- **UDLD:** La detección de link unidireccional es un protocolo de algunas versiones nuevas de software que detecta si la comunicación por un link es únicamente en una dirección. La rotura de un cable de fibra u otros problemas en los cables o el puerto pueden provocar esta comunicación unidireccional. Estos links parcialmente funcionales pueden producir problemas cuando los switches involucrados no conocen que el link está dañado parcialmente. Con este problema, pueden producirse loops de árbol de expansión. El UDLD se puede configurar para poner un puerto en el estado de *errDisable* cuando detecta un link unidireccional.
- **discrepancia de VLAN nativa:** Antes de que un puerto tenga los enlaces troncales activados, pertenece a una sola VLAN. Cuando se activa la conexión troncal, el puerto puede transmitir el tráfico para varias VLAN. El puerto todavía recuerda el VLA N que estaba adentro antes de que el enlace fuera girado, que se llama el VLAN nativo. La VLAN nativa es fundamental para la conexión troncal 802.1q. Si el VLAN nativo en cada extremo del link no hace juego, un puerto entra el estado de *errDisable*.
- **Otro:** Cualquier proceso dentro del Switch que reconoce un problema con el puerto puede colocarlo en el *estado de errDisable*.

Otra causa de los puertos inactivos es la desaparición de la VLAN a la que pertenecen. Cada puerto de un switch pertenece a una VLAN. Si se borra ese VLA N, el puerto llega a estar inactivo. Algunos switches muestran una luz naranja constante en cada puerto en que esto ha

sucedido. Si usted entra trabajar un día y ver los centenares de luces naranja, no se atierre; podría ser que todos los puertos pertenecieron al mismo VLA N y alguien borró accidentalmente el VLA N que los puertos pertenecieron a. Cuando usted agrega el VLA N nuevamente dentro de la tabla de VLAN, los puertos llegan a ser activos otra vez. Un puerto recuerda su VLAN asignado.

Si usted tiene link y los puertos aparecen conectados, pero no puede establecer comunicación con otro dispositivo, esto puede resultar particularmente desconcertante. Generalmente, indica un problema ubicado sobre la capa física: intento de la capa 2 o de la capa 3. estas cosas.

- Verifique el modo de trunking en cada lado del link. Asegúrese a los ambos lados están en el mismo modo. Si usted da vuelta al modo de concentración links a "ON" (en comparación con el "auto" o el "desirable") para un puerto, y el otro puerto tiene el modo de concentración links fijado a "OFF", no pueden comunicar. El enlace cambia el formato del paquete; los puertos necesitan estar en el acuerdo en cuanto a qué formato utilizan en el link o no se entienden.
- Asegúrese de que todos los dispositivos se encuentren en la misma VLAN. Si no están en el mismo VLA N, un router debe ser configurado para permitir que los dispositivos comuniquen.
- Asegúrese de que el direccionamiento de la capa tres esté correctamente configurado.

Problemas de tráfico

En esta sección, describimos algunas de las cosas que usted puede aprender cuando usted mira esa información del tráfico de un puerto. La mayoría de los switches tienen algún modo de realizar el seguimiento de los paquetes que entran y salen de un puerto. Los comandos que generan este tipo de salida en el Switches del Catalyst 4000/5000/6000 son **puerto de la demostración y muestran el mac**. La salida de estos comandos en el Switches de 4000/5000/6000 se describe en las referencias del comando switch.

Algunos de estos campos de acceso de trafico muestran cuántos datos se transmiten y se reciben en el puerto. Otros campos muestran cuántas tramas de errores se encuentran en el puerto. Si usted tiene una gran cantidad de errores de alineación, de errores FCS, o de lateres colisiones, esto puede indicar una discordancia dúplex en el alambre. Las otras causas para estos tipos de errores pueden ser placas de interfaz de red inadecuada o problemas de cable. Si usted tiene un gran número de tramas diferidas, es una muestra que su segmento tiene demasiado tráfico; el Switch no puede enviar bastante tráfico en el alambre para vaciar sus buffers. Considere el retiro de algunos dispositivos a otro segmento.

Falla de hardware del switch

Si usted ha intentado todo que usted puede pensar en y el puerto no trabaja, allí pudo ser hardware defectuoso.

Los puertos son dañados a veces por el Electro-Static Discharge (ESD). Usted puede o no puede ver ninguna indicación de esto.

Vea los resultados de power-on self-test (POST) en el switch para ver si se ha indicado alguna falla para alguna parte del switch.

Si usted ve el comportamiento que se puede solamente considerar "extraño," éste podría indicar los problemas de hardware, pero podría también indicar los problemas del software.

Normalmente, es más sencillo volver a cargar el software que obtener un nuevo hardware. Intente trabajar con el software del switch primero.

El sistema operativo puede tener un error. Si usted carga un más nuevo sistema operativo, podría reparar esto. Usted puede investigar los bug conocido si usted lee los Release Note para la versión del código que usted utiliza o que utiliza el [juego de herramientas del bug Cisco](#).

El sistema operativo habría podido de alguna manera corromperse. Si usted recarga la misma versión del sistema operativo, usted podría reparar el problema.

Si el indicador luminoso de estado en el Switch contellea anaranjado, éste significa generalmente que hay una cierta clase de problema de hardware con el puerto o el módulo o el Switch. La misma cosa es verdad si el puerto o el estado del módulo indica *defectuoso*.

Antes de que usted intercambie el hardware del Switch, usted puede intentar algunas cosas:

- Vuelva a colocar el módulo en el switch. Si hace esto con la energía encendida, asegúrese de que el módulo admita el reemplazo en caliente. En caso de duda, apague el Switch antes de que usted vuelva a sentar el módulo o refiera al guía de instalación del hardware. Si el puerto se incorpora al Switch, ignore este paso.
- Reinicie el switch Esto hace a veces el problema desaparecer; esto es una solución alternativa, no un arreglo.
- Revise el software del switch. Si esto es una nueva instalación, recuerde que algunos componentes pueden trabajar solamente con ciertas versiones del software. Marque los Release Note o la instalación del hardware y la guía de configuración para el componente que usted instala.
- Si usted está razonablemente seguro que usted tiene un problema de hardware, sustituya al componente defectuoso.

[Resolución de problemas de negociación automática half/full duplex de Ethernet 10/100/ Mb](#)

[Objetivos](#)

Esta sección presenta la información de Troubleshooting general y una descripción de las técnicas para resolver problemas la negociación automática de los Ethernetes.

- Esta sección muestra cómo determinar el comportamiento actual de un link. Continúa mostrar cómo los usuarios pueden controlar el comportamiento, así como explica las situaciones cuando la negociación automática falla.
- Muchos Switches Catalyst de Cisco y Routers de Cisco soportan la autonegociación. Esta sección se centra en la negociación automática entre switches Catalyst 5000. Los conceptos explicados aquí se pueden también aplicar a los otros tipos de dispositivos.

[Introducción](#)

La negociación automática es una función opcional de la norma Fast Ethernet de IEEE 802.3u que permite a los dispositivos intercambiar información automáticamente por un link sobre capacidades dúplex y de velocidad.

La negociación automática está destinada a los puertos, los cuales están asignados a los áreas donde los dispositivos o usuarios transitorios se conectan a una red. Por ejemplo, muchas compañías les dan oficinas compartidas o cubículos a sus ejecutivos de cuentas e ingenieros en sistemas para que usen cuando están en la oficina en lugar de en la calle. Cada oficina o cubo tiene un acceso de Ethernet conectado permanentemente con la red de la oficina. Porque no es posible asegurarse de que cada usuario tiene un 10Mb, un Ethernet 100Mb, o un indicador luminoso LED amarillo de la placa muestra gravedad menor 10/100Mb en su laptop, los puertos del switch que manejan estas conexiones deben poder negociar su modo de la velocidad y dúplex. La alternativa puede proporcionar un 10Mb y un puerto 100Mb en cada oficina o cubicularlos y etiquetar por consiguiente.

La negociación automática no se debe utilizar para los puertos que soportan los dispositivos de la infraestructura de red, tales como Switches y Routers u otros sistemas extremos NON-transitorios tales como servidores e impresoras. Aunque la negociación automática para la velocidad y dúplex sea normalmente el comportamiento predeterminado en los puertos del switch que son capaces de él, los puertos conectados con los dispositivos fijos se deben configurar siempre para la conducta correcta bastante que permitidos negociarla. Esto elimina cualquier problema potencial de la negociación y se asegura de que usted sabe siempre exactamente los puertos deben actuar. Por ejemplo, un link entre switches de los Ethernetes 10/100BaseTX que se ha configurado para el Full-duplex 100Mb actúa solamente a esa velocidad y modo. No hay posibilidad de los puertos para retroceder el link a un más despacio dentro de una restauración del puerto o de una restauración del Switch. En caso que los puertos no puedan actuar según lo configurado, no deben pasar ningún tráfico. Por otra parte, un link entre switches que se ha permitido negociar su comportamiento puede actuar en el half duplex 10Mb. Un link no funcional es generalmente más fácil de descubrir que un link, que es operativo, pero no actúa a la velocidad o al modo prevista.

Una de la mayoría de las causas comunes de los problemas de rendimiento en los links Ethernet 10/100Mb es cuando un puerto en el link actúa en el half duplex, mientras que el otro puerto actúa en por completo - duplex. Esto sucede de vez en cuando cuando un o ambo puertos en un link se reajustan y el proceso de negociación automática no da lugar a ambos partners de link que tengan la misma configuración. También sucede cuando los usuarios vuelven a configurar sólo un lado de un link y se olvidan de volver a configurar el otro lado. Se evitan muchos visita de personal técnico por problemas de rendimiento si usted crea una directiva que requiera los puertos para que todos los dispositivos NON-transitorios sean configurados para su comportamiento requerido y aplica la directiva con las medidas adecuadas del control de cambios.

[Resolución de la negociación automática de Ethernet entre los dispositivos de infraestructura de la red](#)

[Procedimientos y/o escenarios](#)

Cat 5k del escenario 1. con los fast ethernet

Cuadro 22-2: Problemas de conectividad de la negociación automática

Posible problema	Solución
¿El	1. Para determinar el comportamiento actual

comportamiento actual del auto del link fue negociado?	de un link, utilice el comando show port mod_num/port_num. Si ambos partners de link (interfaces en cualquier extremo del link) indican tenga un prefijo "a" en su duplex y los campos de estado de velocidad, negociación automática eran probablemente acertados.
Negociación automática no soportada.	2. Publique el mod_num de las capacidades de puerto de la demostración/el comando del port_num de verificar que sus módulos soportan la negociación automática.
La negociación automática no trabaja en los switches de Catalyst.	3. Utilice el mod_num de la velocidad del set port/el comando auto del port_num en un Catalyst de configurar la negociación automática. 4. Intente los diversos puertos o módulos. 5. Intente reajustar los puertos. 6. Intente diversos cables de interconexiones. 7. Devuelva los dispositivos apagado y encendido otra vez.
La negociación automática no trabaja en los routers Cisco.	8. Publique el comando ios correcto de habilitar la negociación automática (si está disponible) 9. diversas interfaces del intento. 10. Intente reajustar las interfaces. 11 Intente diversos cables de interconexiones. 12. Devuelva los dispositivos apagado y encendido otra vez.

[Ejemplo de configuración y resolución de problemas de negociación automática de Ethernet de 10/100 Mb.](#)

Esta sección del documento recorre usted con el examen del comportamiento de un acceso de Ethernet 10/100Mb que soporte la negociación automática. También muestra cómo realizar los cambios a su comportamiento predeterminado y cómo restablecerlo al comportamiento predeterminado.

Tareas se realizan que

1. Examine las capacidades de los puertos.
2. Configure la negociación automática para el puerto 1/1 en ambos switches.
3. Determine si el modo velocidad y dúplex están configurados en negociación automática.
4. Cambie la velocidad en el puerto 1/1 en el Switch A a 10Mb.
5. Comprenda el significado del prefijo "a-" en el dúplex y los campos de estado de velocidad.
6. Vea el estado dúplex del puerto 1/1 en el switch B.
7. Interprete el error de discordancia dúplex.

8. Interprete los mensajes de error del spanning tree.
9. Cambie el modo dúplex a semidúplex en el puerto 1/1 del Switch A.
10. Configure el modo dúplex y la velocidad del puerto 1/1 en el switch B.
11. Restaure el modo de dúplex y la velocidad predeterminados en los puertos 1/1 en ambos switches.
12. Vea los cambios del estado del puerto en ambos switches.

Paso a paso

Siga estos pasos:

1. El comando `show port 1/1 capabilities` muestra las capacidades de un puerto Ethernet 10/100BaseTX 1/1 en el switch A. Ingrese este comando para ambos puertos que usted resuelve problemas. Ambos puertos deben soportar las capacidades de la velocidad y dúplex mostradas si se suponen para utilizar la negociación automática.

```
Switch-A> (enable) show port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half,full
```

2. La negociación automática se configura para ambos modo de la velocidad y dúplex en el puerto 1/1 de ambo Switches si usted ingresa el **comando set port speed 1/1 auto** (el auto es el valor por defecto para los puertos que soportan la negociación automática).

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A (enable)
```

Note: El comando `set port speed {mod_num/port_num} auto` también fija el modo dúplex para auto. No existe ningún comando `set port duplex {mod_num/port_num} auto`.

3. El comando `show port 1/1` visualiza el estatus de los puertos 1/1 enciende A y el B.

```
Switch-A> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal a-full a-100 10/100BaseTX
```

```
Switch-B> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal a-full a-100 10/100BaseTX
```

Observe que la mayor parte del resultado normal del comando `show port {mod_num/port_num}` ha sido omitido. Los prefijos "a-" en "full" y "100" indican que este puerto no se ha definido (configurado) para una velocidad o modo dúplex específico. Por lo tanto puede automáticamente negocia su modo dúplex y velocidad si puede el dispositivo él está conectado con (su partner de link) también automáticamente negocia su modo dúplex y velocidad. También observe que el estado es "connected" (conectado) en ambos puertos, lo que significa que el otro puerto ha detectado un pulso de link. El estado puede ser "conectado" aún si el dúplex ha sido negociado incorrectamente o mal configurado.

4. Para demostrar qué sucede cuando un partner de link es negociación auto y no es el otro partner de link, la velocidad en el puerto 1/1 en el Switch A se fija a 10Mb con el **comando**

set port speed 1/1 10.

```
Switch-A> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-A> (enable)
```

Note: Si usted código duro la velocidad en un puerto, él inhabilita toda la funcionalidad de negociación automática en el puerto para la velocidad y dúplex. Cuando un puerto se ha configurado para una velocidad, configuran a su modo dúplex automáticamente para el modo que había negociado previamente; en este caso, por completo - duplex. Cuando usted ingresa el **comando set port speed 1/1 10** hizo al modo dúplex en el puerto 1/1 ser configurado como si hubieran ingresado al comando **set port duplex 1/1 full** también. Esto se explica después.

5. Entienda el significado del prefijo "a" en el duplex y los campos de estado de velocidad. La ausencia de la "a" prefijo en los campos de estatus de la salida del **comando show port 1/1** en el Switch A muestra que ahora configuran al modo dúplex para "por completo," y la velocidad ahora se configura para el "10."

```
Switch-A> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal full   10   10/100BaseTX
```

6. El comando **show port 1/1** en el switch B indica que el puerto ahora actúa en el half duplex y 10Mb.

```
Switch-B> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal a-half a-10  10/100BaseTX
```

Este paso muestra que es posible que un partner de link detecte la velocidad a la que opera el otro partner de link a pesar de que el otro partner de link no esté configurado para la negociación automática. La detección del tipo de señal eléctrica que esté llegando para considerar si es 10Mb o 100Mb hace esto. Éste es cómo el switch B determinó que el puerto 1/1 debe actuar en 10Mb. No es posible detectar el modo dúplex correcto de la misma forma que se puede detectar la velocidad correcta. En este caso, donde el puerto de 1/1 de switch B se configura para la negociación automática y no es el puerto de Switch A, el puerto de 1/1 de switch B fue forzado para seleccionar al modo dúplex predeterminado. En los puertos Catalyst Ethernet, el modo predeterminado es negociación automática y si este modo falla, entonces es semi dúplex. Este ejemplo también muestra que un link puede ser conectado exitosamente cuando no coinciden los modos de dúplex. El puerto 1/1 del switch A está configurado para dúplex completo, mientras que el puerto 1/1 del switch B está configurado de manera predeterminada en medio dúplex. Para evitar esto, configure siempre a ambos partners de link. El prefijo "a-" en los campos de estado Duplex (Dúplex) y Speed (Velocidad) no siempre significa que se ha negociado el comportamiento actual. A veces sólo significa que el puerto no ha sido configurado para velocidad o modo dúplex. El resultado anterior del Switch B muestra al dúplex como "a-half" (semi) y la velocidad como "a-10" lo que indica que el puerto está funcionando a 10 Mb en modo semidúplex. En este ejemplo, el partner de link en este puerto (el puerto 1/1 en el Switch A) se configura para "por completo" y el "10Mb." no era posible para el puerto 1/1 en el switch B tener automáticamente negociado su comportamiento actual. Esto prueba que el prefijo "a" indica solamente una buena voluntad de realizar la negociación automática - no esa negociación automática ocurrió realmente.

7. Entienda el mensaje de error de discordancia dúplex. Este mensaje sobre una discordancia del modo dúplex se visualiza en el Switch A después de que la velocidad en el puerto 1/1 fuera cambiada a 10Mb. La discordancia fue causada por el puerto de 1/1 de switch B, que omiten el half duplex porque detectaron a su partner de link podrían realizar no más la negociación automática.

```
%CDP-4-DUPLEXMISMATCH:Full/half duplex mismatch detected 01
```

Es importante tener en cuenta que a este mensaje lo crea el Protocolo de detección de Cisco (CDP), y no el protocolo de negociación automática 802.3. El CDP puede señalar los problemas que descubre, pero no los repara típicamente automáticamente. Una discordancia dúplex puede o no puede dar lugar a un mensaje de error. Otra señal de una discordancia dúplex es un aumento rápido de errores de alineación y FCS en el lado del semi dúplex y "fragmentos minúsculos" en el puerto dúplex completo (tal como se ve en un puerto sh {mod_num/port_num}).

8. Entienda los mensajes del Spanning-tree. Además del mensaje de error de discordancia dúplex, usted puede también ver estos mensajes del Spanning-tree cuando usted cambia la velocidad en un link. Una discusión del Spanning-tree está fuera del alcance de este documento; refiera el capítulo en el Spanning-tree para más información sobre el Spanning-tree.

```
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
```

```
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1
```

9. Para demostrar qué sucede cuando han configurado al modo dúplex, el modo en el puerto 1/1 en el Switch A se fija a la mitad con el **comando set port duplex 1/1 half**.

```
Switch-A> (enable) set port duplex 1/1 half
```

```
Port(s) 1/1 set to half-duplex.
```

```
Switch-A> (enable)
```

El comando show port 1/1 muestra el cambio en el modo Duplex en este puerto.

```
Switch-A> (enable) sh port 1/1
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
1/1		connected	1	normal	half	10	10/100BaseTX

En este momento, los puertos 1/1 en ambo Switches están actuando en el half duplex. El puerto 1/1 en el switch B todavía se configura al auto negocia, tal y como se muestra en de esta salida del **comando show port 1/1**.

```
Switch-B> (enable) show port 1/1
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
1/1		connected	1	normal	a-half	a-10	10/100BaseTX

Este paso muestra cómo configurar al modo dúplex en el puerto 1/1 en el switch B a la mitad. Esto es constante con la política recomendada configurar a ambos partners de link de la misma manera.

10. Para implementar la directiva a las maneras configure a ambos partners de link para el mismo comportamiento, este paso ahora fija al modo dúplex a la mitad y a la velocidad a 10 en el puerto 1/1 en el switch B. Aquí está el resultado del ingreso del comando set port duplex 1/1 half en el switch B:

```
Switch-B> (enable) set port duplex 1/1 half
```

```
Port 1/1 is in auto-sensing mode.
```

```
Switch-B> (enable)
```

El comando **set port duplex 1/1 half** falló porque este comando es inválido si se habilita la negociación automática. Esto también significa que este comando no inhabilita la negociación automática. La negociación automática se puede inhabilitar solamente con el **set port speed {mod_num/port_num {10 | 100}}** .Aquí está el resultado de la ejecución del comando **set port speed 1/1 10** en el switch B.

```
Switch-B> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-B> (enable)
```

Ahora el comando **set port duplex 1/1 half** en los trabajos del switch B:

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

El comando **show port 1/1** en el switch B muestra que el puerto ahora está configurado para semidúplex y 10 Mb.

```
Switch-B> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal half   10   10/100BaseTX
```

Note: El comando **set port duplex {mod_num/port_num {half | full}}** depende en el comando **set port speed {mod_num/port_num {10 | 100}}** . En otras palabras, debe configurar la velocidad antes de activar el modo dúplex.

11. Configure los puertos 1/1 en ambos switches para que negocien en forma automática con el comando **set port speed 1/1 auto**.

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A> (enable)
```

Note: Han configurado una vez a un modo dúplex de un puerto algo con excepción del auto, la única forma de configurar el puerto a la detección automática que su modo dúplex es publicar el comando **set port speed {mod_num/port_num} auto**. No existe ningún comando **set port duplex {mod_num/port_num} auto**. Es decir si usted publica el comando **set port speed {mod_num/port_num} auto**, reajusta la velocidad de puerto que detecta y detección de modo dúplex al auto.

12. Examine el estatus de los puertos 1/1 en ambo Switches con el comando **show port 1/1**.

```
Switch-A> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal a-full a-100 10/100BaseTX
Switch-B> (enable) show port 1/1
Port Name          Status      Vlan      Level Duplex Speed Type
-----
1/1                connected  1         normal a-full a-100 10/100BaseTX
```

Ahora, ambos puertos están configurados con su comportamiento predeterminado de auto negociación. Ambos puertos han negociado el dúplex completo y 100Mb.

[Antes de que usted llame el equipo de Soporte técnico de Cisco Systems](#)

Antes de que usted llame el sitio web del Soporte técnico de Cisco Systems, asegúrese le haber leído con este capítulo y haber completado las acciones sugeridas para su problema de sistema.

Además, haga éstos y documente los resultados de modo que poder ayudarle mejor:

- Capture la salida de la **versión de la demostración de** todos los dispositivos afectados.
- Capture la salida del **show port mod_num/port_num de** todos los puertos afectados.
- Capture el resultado de **show port mod_num/port_num capabilities** desde todos los puertos afectados.

[Configuración de las conexiones switch-a-switch EtherChannel de los switches Catalyst 4000/5000/6000](#)

EtherChannel permite la combinación de múltiples links físicos Fast Ethernet o Gigabit Ethernet en un canal lógico. Esto permite que el tráfico entre los links sean distribuidos la carga en el canal, así como la Redundancia en caso que uno o más links en el canal fallen. El EtherChannel se puede utilizar para interconectar los switches LAN, Routers, los servidores, y los clientes con la conexión del par trenzado sin blindaje (UTP) o modo simple y fibra de modos múltiples.

EtherChannel es una manera fácil de agregar ancho de banda entre dispositivos de red críticos. En el Catalyst 5000, un canal se puede crear a partir de dos puertos que le hagan un link 200Mbps (FULL-duplex 400Mbps) o de cuatro puertos que le hagan un link 400Mbps (FULL-duplex 800Mbps). Algunas tarjetas y plataformas también admiten Gigabit EtherChannel y tienen la capacidad de utilizar entre dos y ocho puertos en un EtherChannel. El concepto es el mismo sin importar las velocidades o la cantidad de links involucrados. El Spanning Tree Protocol (STP) considera estos links redundantes entre dos dispositivos ser loops y hace normalmente los links redundantes estar en el modo de bloqueo, que con eficacia hace estos links inactivos (que proporcione solamente las capacidades de backup si el link principal falla). Cuando usted utiliza IOS 3.1.1 o mayor, atravesando - el árbol trata el canal como un gran link, así que todos los puertos en el canal pueden ser activos al mismo tiempo.

Esta sección le toma con los pasos para configurar el EtherChannel entre dos Catalyst 5000 Switch y para mostrarle los resultados de los comandos mientras que se ejecutan. Los Catalyst 4000 y 6000 Switches se habrían podido utilizar en los escenarios presentados en este documento para obtener los mismos resultados. Para el Catalyst 2900XL y el 1900/2820, la sintaxis de los comandos es diferente, pero los conceptos EtherChannel son lo mismo.

El EtherChannel puede ser configurado manualmente si usted teclea adentro los comandos apropiados, o puede ser configurado automáticamente si el Switch negocia el canal con el otro lado con el Port Aggregation Protocol (PAgP). Se recomienda para utilizar el desirable mode del PAgP para configurar el EtherChannel siempre que sea posible puesto que la configuración manual del EtherChannel puede crear algunas complicaciones. Este documento da los ejemplos de cómo configurar el EtherChannel manualmente y los ejemplos de cómo configurar el EtherChannel con el PAgP. También se incluye cómo resolver problemas de EtherChannel y cómo usar el enlace troncal con EtherChannel. En este documento, el EtherChannel de los términos, Fast EtherChannel, Gigabit EtherChannel o canaliza todo refiere al EtherChannel.

Contenido

1. [Tareas para la configuración manual del EtherChannel](#)
2. [Verifique la configuración de EtherChannel](#)
3. [Utilice el PAgP para configurar automáticamente el EtherChannel \(el método preferido\)](#)
4. [Enlace troncal y EtherChannel](#)

5. [Resolución de problemas de EtherChannel](#)
6. [Comandos usados en este documento](#)

Esta figura ilustra nuestro entorno de prueba. La configuración de los Switches se ha borrado con el comando `clear config all`. Entonces, el prompt fue cambiado con el **nombre del sistema del conjunto**. Una dirección IP y una máscara fueron asignadas al Switch para los fines de administración con el `int sc0 172.16.84.6 255.255.255.0` del conjunto para el `int sc0 172.16.84.17 255.255.255.0` de SwitchA y del conjunto para SwitchB. Un default gateway fue asignado a ambos Switches con el `set ip route default 172.16.84.1`.

Se borraron las configuraciones de switch para poder comenzar con las condiciones predeterminadas. A los switches se les asignaron nombres que permitieran identificarlos en la indicación de la línea de comandos. Los IP Addresses fueron asignados de modo que pudiéramos hacer ping entre los Switches para probar. No se usó la gateway predeterminada.

Muchos de los comandos muestran más resultados de los necesarios para el tratamiento de este tema. La salida extraña se borra en este documento.

[Tareas para la configuración manual del EtherChannel](#)

Esto es una sinopsis de las direcciones para configurar manualmente el EtherChannel.

1. [Muestre la versión de IOS y los módulos que utilizamos en este documento.](#)
2. [Verifique la compatibilidad de EtherChannel con los puertos.](#)
3. [Verifique que los puertos se encuentren conectados y en funcionamiento.](#)
4. [Verifique que los puertos a agrupar tengan la misma configuración.](#)
5. [Identifique grupos de puertos válidos.](#)
6. [Cree el canal](#)

[Paso a paso](#)

Éstos son los pasos para configurar manualmente el EtherChannel.

1. El comando `show version` visualiza la versión de software que el Switch funciona con. El comando `show module` enumera los módulos que están instalados en el switch.

```
Switch-A show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
?
```

```
Switch-A show module
Mod Module-Name          Ports Module-Type          Model      Serial-Num Status
-----
1                0      Supervisor III           WS-X5530   006841805 ok
2                24     10/100BaseTX Ethernet  WS-X5225R  012785227 ok
?
```

2. Verifique que EtherChannel está soportado en los puertos, muestre las capacidades de los puertos aparece en las versiones 4.x y superiores. Si cuenta con una versión de IOS anterior a 4.x, debe saltar este paso. No todos los módulos Fast Ethernet admiten EtherChannel. Algunos de los módulos EtherChannel tienen "Fast EtherChannel" escrito en la esquina inferior izquierda del módulo (como se ve en el switch) lo que significa que la función es

admitida. Abandonaron a este convenio en módulos posteriores. Los módulos en esta prueba no tienen "Fast EtherChannel" impreso en ellos, pero son compatibles con la función.

```
Switch-A show port capabilities
Model                WS-X5225R
Port                 2/1
Type                 10/100BaseTX
Speed                auto,10,100
Duplex               half,full
Trunk encap type     802.1Q,ISL
Trunk mode            on,off,desirable,auto,nonegotiate
Channel              2/1-2,2/1-4
Broadcast suppression percentage(0-100)
Flow control          receive-(off,on),send-(off,on)
Security              yes
Membership            static,dynamic
Fast start            yes
Rewrite               yes
Switch-B show port capabilities
Model                WS-X5234
Port                 2/1
Type                 10/100BaseTX
Speed                auto,10,100
Duplex               half,full
Trunk encap type     802.1Q,ISL
Trunk mode            on,off,desirable,auto,nonegotiate
Channel              2/1-2,2/1-4
Broadcast suppression percentage(0-100)
Flow control          receive-(off,on),send-(off,on)
Security              yes
Membership            static,dynamic
Fast start            yes
Rewrite               no
```

Un puerto que no soporta los parecer del EtherChannel esto.

```
Switch show port capabilities
Model                WS-X5213A
Port                 2/1
Type                 10/100BaseTX
Speed                10,100,auto
Duplex               half,full
Trunk encap type     ISL
Trunk mode            on,off,desirable,auto,nonegotiate
Channel              no
Broadcast suppression pps(0-150000)
Flow control          no
Security              yes
Membership            static,dynamic
Fast start            yes
```

3. Verifique que los puertos se encuentren conectados y en funcionamiento. Antes de que usted conecte los cables, éste es el estado del puerto.

```
Switch-A show port
Port Name           Status      Vlan      Level Duplex Speed Type
-----
2/1                 notconnect 1          normal  auto  auto 10/100BaseTX
2/2                 notconnect 1          normal  auto  auto 10/100BaseTX
2/3                 notconnect 1          normal  auto  auto 10/100BaseTX
2/4                 notconnect 1          normal  auto  auto 10/100BaseTX
```

Después de que usted conecte los cables entre el dos Switches, éste es el estatus.

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
```

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4
```

```
Switch-A show port
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1		connected	1	normal	a-full	a-100	10/100BaseTX
2/2		connected	1	normal	a-full	a-100	10/100BaseTX
2/3		connected	1	normal	a-full	a-100	10/100BaseTX
2/4		connected	1	normal	a-full	a-100	10/100BaseTX

```
Switch-B show port
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1		connected	1	normal	a-full	a-100	10/100BaseTX
2/2		connected	1	normal	a-full	a-100	10/100BaseTX
2/3		connected	1	normal	a-full	a-100	10/100BaseTX
2/4		connected	1	normal	a-full	a-100	10/100BaseTX

Puesto que las configuraciones del switch fueron borradas antes de que esta prueba comenzada, los puertos esté en sus condiciones predeterminadas. Son todas en el vlan1, y su velocidad y dúplex se fija al auto. Después de la conexión de los cables, negocian a una velocidad de 100Mbps y por completo - duplex. El estatus está conectado, así que podemos hacer ping el otro Switch.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

En su red, usted puede ser que quiera a fijar las velocidades manualmente a 100Mbps y por completo - duplex en vez de la confianza en la negociación automática puesto que usted quisiera probablemente que sus puertos se ejecutaran siempre en la máxima velocidad. Para una explicación de la negociación automática, vea la [mitad/la negociación automática del dúplex completo y del semidúplex de los Ethernetes 10/100Mb del troubleshooting de la sección](#).

4. Verifique que los puertos a agrupar tengan la misma configuración. Éste es un punto importante que se cubre más detalladamente en la sección de Troubleshooting. Si el comando de poner el EtherChannel no trabaja, está generalmente porque los puertos implicados en el canal tienen configuraciones que diferencien de uno a. Esto incluye los puertos en el otro lado del link, así como los puertos locales. En nuestro caso, puesto que las configuraciones del switch fueron borradas antes de que esta prueba comenzada, los puertos esté en sus condiciones predeterminadas. Son todas en el vlan1; su velocidad y dúplex se fija al auto, y a todo el atravesar - los parámetros del árbol para cada puerto se fijan lo mismo. Vimos de la salida que después de que los cables estén conectados, los puertos negocia a una velocidad de 100Mbps y por completo - duplex. Puesto que atravesando - el árbol se ejecuta para cada VLA N, es más fácil apenas configurar el canal y responder a los mensajes de error que intentar y marcar cada atravesar - el árbol coloque para el estado coherente para cada puerto y el VLA N en el canal.
5. Identifique grupos de puertos válidos. En el Catalyst 5000, solamente los ciertos puertos se pueden poner juntos en un canal. Estas dependencias restrictivas no se aplican a todas las plataformas. Los puertos en un canal en un Catalyst 5000 deben ser contiguos. Aviso del **comando show port capabilities** que para el puerto 2/1, éstas son las combinaciones posible.:

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```


Tenga en cuenta que este puerto puede formar parte de un grupo de dos (2/1-2) o parte de un grupo de cuatro (2/1-4). Hay algo llamado un Controlador de agrupación de Ethernet (EBC) en el módulo que causa estas limitaciones de la configuración. Observemos otro puerto.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

Este puerto se puede agrupar en un grupo de dos puertos (2/3-4) o en un grupo de cuatro (2/1-4). **Note:** El dependiente sobre el hardware, allí puede ser restricciones adicionales. En los módulos determinados (WS-X5201 y WS-X5203), usted no puede formar un EtherChannel con los dos puertos más recientes de un “grupo de puertos” a menos que los primeros dos puertos en el grupo formen ya un EtherChannel. Un “grupo de puertos” es un grupo de puertos se permite que formar un EtherChannel (2/1-4 es un grupo de puertos en este ejemplo). ¡Por ejemplo, si usted crea los EtherChanneles separados con solamente dos puertos en un canal, usted no puede asignar a los puertos 2/3-4 a un canal hasta que usted tenga primeros puertos configurados 2/1-2 a un canal, para los módulos que tienen esta restricción! Asimismo, antes de que usted configure los puertos 2/6-7, usted debe configurar los puertos 2/5-6. Esta restricción no ocurre en los módulos usados para este documento (WS-X5225R, WS-X5234). Puesto que configuramos un grupo de cuatro puertos (2/1-4), esto está dentro del agrupamiento aprobado. No podemos asignar a un grupo de cuatro a los puertos 2/3-6. Esto es un grupo de puertos contiguos, pero no comienzan en el límite aprobado, como se muestra por el **comando show port capabilities** (los grupos válidos serían puertos 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

6. Cree el canal Para crear el canal, utilice el comando **set port channel <mod/port encendido** para cada Switch. Recomendamos que usted da vuelta a los puertos apagado en el un lado del canal o el otro lado con el **comando set port disable** antes de que usted gire el EtherChannel manualmente. Esto evita los Posibles problemas con atravesar - árbol dentro del proceso de configuración. El Spanning-tree puede apagar algunos puertos (con un estado del puerto de “errdisable”) si se configura un lado mientras que un canal antes de que el otro lado se pueda configurar como canal. Debido a esta posibilidad, es mucho más fácil crear los EtherChanneles con el PAgP, que se explica más adelante en este documento. Para evitar esta situación cuando usted configura el EtherChannel manualmente, inhabilitamos los puertos en SwitchA, configuramos el canal en SwitchA, configuramos el canal en SwitchB, y después volvemos a permitir los puertos en SwitchA. En primer lugar, verifique que la canalización esté desconectada.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

Ahora inhabilite los puertos en SwitchA hasta que ambo Switches se haya configurado para el EtherChannel de modo que atravesando - el árbol no genera los errores y apaga los puertos.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

Dé vuelta al modo del canal a *encendido* para SwitchA.

```
Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verifique el estado del canal. Note que han fijado al modo del canal a *encendido*, solamente

el estatus de los puertos se inhabilita (porque inhabilitamos entonces anterior). El canal no es operativo en este momento, sino que llega a ser operativo cuando se habilitan los puertos.

```
Switch-A (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

Dado que los puertos del switch A estuvieron (temporalmente) desactivados, los puertos del switch B ya no tienen una conexión. Este mensaje se visualiza en la consola de SwitchB cuando los puertos de SwitchA fueron inhabilitados.

```
Switch-A (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

Gire el canal para el switch B.

```
Switch-B (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

Verifique que el modo del canal esté encendido para SwitchB.

```
Switch-B (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

Note que el modo del canal para SwitchB está encendido, solamente el estatus de los puertos es *notconnect*. Esto se debe a que los puertos del SwitchA todavía están desactivados. Finalmente, el último paso es activar los puertos en el SwitchA.

```
Switch-B (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

Verifique la Configuración

Para verificar que el canal esté puesto correctamente, haga el comando **show port channel**.

```
Switch-B (enable) set port channel 2/1-4 on  
Port(s) 2/1-4 channel mode set to on.
```

El Spanning-tree se muestra para tratar los puertos como un puerto lógico en este comando. Cuando el puerto se enumera como *2/1-4*, atravesando - el árbol está tratando los puertos 2/1, 2/2, 2/3 y 2/4 como *un puerto*.

```
Switch-A (enable) show spantree  
VLAN 1  
Spanning tree enabled  
Spanning tree type          ieee  
  
Designated Root             00-10-0d-b2-8c-00  
Designated Root Priority    32768  
Designated Root Cost        8  
Designated Root Port        2/1-4  
Root Max Age 20 sec        Hello Time 2 sec        Forward Delay 15 sec  
  
Bridge ID MAC ADDR          00-90-92-b0-84-00  
Bridge ID Priority           32768  
Bridge Max Age 20 sec        Hello Time 2 sec        Forward Delay 15 sec
```

Port	Vlan	Port-State	Cost	Priority	Fast-Start	Group-Method
2/1-4	1	forwarding	8	32	disabled	channel

El EtherChannel se puede implementar con diversas maneras de distribución del tráfico a través de los puertos en un canal. La especificación EtherChannel no impone cómo debe distribuirse el tráfico en los links dentro de un canal. El Catalyst 5000 utiliza el bit más reciente o los dos bits más recientes (dependientes sobre cuántos links están en el canal) de los MAC Address de origen y destino en la trama para determinar que viran hacia el lado de babor en el canal para utilizar. Usted ve las cantidades de tráfico similares en cada uno de los puertos en el canal si ese tráfico es generado por una distribución normal de las direcciones MAC en un lado del canal o el otro. Para verificar que el tráfico pase todos los puertos en el canal, usted puede utilizar el **comando show mac**. Si sus puertos eran activos antes de que usted configurara el EtherChannel, usted puede reajustar a los contadores de tráfico a cero del **comando clear counters**, y entonces los valores de tráfico representan cómo el EtherChannel ha distribuido el tráfico.

En nuestro entorno de prueba, no conseguimos una distribución del mundo real porque no hay puestos de trabajo, servidores, o Routers que genera el tráfico. Los únicos dispositivos que generan el tráfico son el Switches ellos mismos. Publicamos algunos ping de SwitchA a SwitchB, y usted puede decir que el tráfico de unidifusión utiliza el primer puerto en el canal. La información de recepción en este caso (unidifusión Rcv) muestra cómo el Switch B distribuyó el tráfico a través del canal hasta el Switch A. Un poco más bajo en la salida, la información del transmitir (Xmit-unicast) muestra cómo SwitchA distribuyó el tráfico a través del canal a SwitchB. También vemos que sale un muy poco de tráfico Multicast Switch-generado (ISL dinámico, CDP) los cuatro puertos. Los paquetes de broadcast son interrogaciones ARP (para el default gateway - que no existe en nuestro laboratorio aquí). Si tuviéramos puestos de trabajo que envían los paquetes a través del Switch a un destino en el otro lado del canal, esperábamos ver el tráfico que pasa cada uno de los cuatro links en el canal. Usted puede monitorear la distribución de paquetes en su propia red con el **comando show mac**.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Switch-A (enable) show mac
```

Port	Rcv-Unicast	Rcv-Multicast	Rcv-Broadcast
2/1	9	320	183
2/2	0	51	0
2/3	0	47	0
2/4	0	47	0
(...)			

Port	Xmit-Unicast	Xmit-Multicast	Xmit-Broadcast
2/1	8	47	184
2/2	0	47	0
2/3	0	47	0
2/4	0	47	0
(...)			

Port	Rcv-Octet	Xmit-Octet
2/1	35176	17443
2/2	5304	4851
2/3	5048	4851

Last-Time-Cleared

Wed Dec 15 1999, 01:05:33

Utilice el PAgP para configurar el EtherChannel (el método preferido)

El Port Aggregation Protocol (PAgP) facilita la creación automática de los links EtherChannels con el intercambio de los paquetes entre los puertos aptos para canal. El protocolo aprende las capacidades de los grupos de puertos dinámicamente e informa a los puertos próximos.

Una vez que PAgP identifica los links channel-capable que pueden juntarse correctamente, agrupa los puertos en un canal. El canal luego se agrega al árbol de expansión como un solo puerto de puente. Un paquete de difusión o de multidifusión de salida determinado se transmite sólo a un puerto del canal y no a todos los puertos del canal. Además, los broadcastes salientes y paquetes de multicast transmitidos en un puerto en un canal se bloquean de su vuelta en cualquier otro puerto del canal.

Existen cuatro modos de canal que el usuario puede configurar: en, apagado, auto, y deseable. Los paquetes PagP sólo se intercambian entre puertos en los modos Auto y Desirable. Los puertos configurados en modo conectado o desconectado no intercambian paquetes PagP. La configuración recomendada para los switches que formarán un EtherChannel, es tener ambos configurados al modo deseado. Esto proporciona el comportamiento más contundente que debería encontrar situaciones de error de un lado o del otro o bien reiniciar. El modo predeterminado del canal es automático.

Ambos los **modos Autos y Desirable** permiten que los puertos negocien con los puertos conectados para determinar si pueden formar un canal basado en los criterios tales como velocidad de puerto, estado de troncal, VLAN nativo, etc.

Los puertos pueden formar un EtherChannel cuando están en diversos modos del canal mientras los modos sean compatibles:

- Un puerto en modo deseable puede formar un EtherChannel exitosamente con otro puerto que se encuentre en el modo deseable o automático.
- Un puerto en modo automático puede formar un EtherChannel con otro puente en el modo que se desee.
- Un puerto en el **modo automático** no puede formar un EtherChannel con otro puerto que esté también en el **modo automático** puesto que ninguno puerto inicia la negociación.
- Un puerto adentro **en el** modo puede formar un canal solamente con un puerto adentro **en el** modo porque los puertos adentro **en el** modo no intercambian los paquetes PAgP.
- Un puerto en el **modo desconectado** no forma un canal con ningún puerto.

Cuando usted utiliza el EtherChannel, si un "SPANTREE-2: "Channel misconfig - x/x-x will be disabled" (Configuración errónea del canal - x/x-x se inhabilitará) o un mensaje syslog similar aparece en pantalla, esto indica una discordancia de modos EtherChannel en los puertos conectados. Recomendamos que usted corrija la configuración y volvemos a permitir los puertos con el **comando set port enable**. Las configuraciones de EtherChannel válidas incluyen éstos:

Tabla 22-5: Configuraciones válidas de EtherChannel

Modo de canal de puerto	Modo(s) de canal del puerto de vecino válido(s)
deseable	deseable o automático
auto (default)	deseable o automático ¹
encendido	encendido
desactivado	desactivado

¹ Si el local y los puertos de vecino están en el **modo automático**, un agrupamiento de EtherChannel no forman.

Aquí está un resumen de todos los escenarios de modo de canalización posibles. Algunas de estas combinaciones pueden causar atravesar - árbol para poner los puertos en el lado de canalización en el *estado de errDisable* (es decir, cerrado les).

Tabla 22-6: Escenarios de modo de canalización

Modo de Canal de Switch-A	Modo de Canal del Switch B	Estado del Canal
Encendido	Encendido	Canal
Encendido	Desactivado	No canal (errdisable)
Encendido	Auto	No canal (errdisable)
Encendido	Deseable	No canal (errdisable)
Desactivado	Encendido	No canal (errdisable)
Desactivado	Desactivado	Sin Canal
Desactivado	Auto	Sin Canal
Desactivado	Deseable	Sin Canal
Auto	Encendido	No canal (errdisable)
Auto	Desactivado	Sin Canal
Auto	Auto	Sin Canal
Auto	Deseable	Canal
Deseable	Encendido	No canal (errdisable)
Deseable	Desactivado	Sin Canal
Deseable	Auto	Canal
Deseable	Deseable	Canal

Apagamos el canal del ejemplo anterior con este comando en SwitchA y SwitchB.

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
```

El modo de canal predeterminado de un puerto capaz de canalizar es automático. Para verificar

esto ingrese este comando.

```
Switch-A (enable) show port channel 2/1
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	auto	not channel		

El comando anterior también muestra que los puertos no canalizan actualmente. Otra manera de verificar al estado del canal es ésta.

```
Switch-A (enable) show port channel
```

```
No ports channelling
```

```
Switch-B (enable) show port channel
```

```
No ports channelling
```

Es realmente muy simple hacer que el canal trabaje con el PAgP. En este momento ambos Switches se fija al modo automático que significa que él canaliza si un puerto conectado envía una petición del PAgP de canalizar. Si usted setSwitchA a deseable, SwitchA, él hace SwitchA enviar los paquetes PAgP al otro Switch y lo pide para canalizar.

```
Switch-A (enable) set port channel 2/1-4 desirable
```

```
Port(s) 2/1-4 channel mode set to desirable.
```

```
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 22:03:24 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Para ver el canal, haga esto.

```
Switch-A (enable) show port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	desirable channel		WS-C5505	066509957 (Sw 2/1)
2/2	connected	desirable channel		WS-C5505	066509957 (Sw 2/2)
2/3	connected	desirable channel		WS-C5505	066509957 (Sw 2/3)
2/4	connected	desirable channel		WS-C5505	066509957 (Sw 2/4)

Puesto que SwitchB estaba en el modo automático, respondió a los paquetes PAgP y creó un canal con SwitchA.

```
Switch-B (enable)
```

```
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
```

```
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
```

```

2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 14 20:26:48 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

```

```
Switch-B (enable) show port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	auto	channel	WS-C5505	066507453 (Sw 2/1
2/2	connected	auto	channel	WS-C5505	066507453 (Sw 2/2
2/3	connected	auto	channel	WS-C5505	066507453 (Sw 2/3
2/4	connected	auto	channel	WS-C5505	066507453 (Sw 2/4

Note: Se recomienda para fijar los ambos lados del canal a **deseable** de modo que los ambos lados intenten iniciar el canal si un lado sale. Si usted fija los puertos EtherChannel en SwitchB al **desirable mode**, aunque el canal está actualmente - active y en el **modo automático**, no plantea ningún problema. Éste es el comando.

```
Switch-B (enable) set port channel 2/1-4 desirable
```

```
Port(s) 2/1-4 channel mode set to desirable.
```

```
Switch-B (enable) show port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	desirable	channel	WS-C5505	066507453 (Sw 2/1
2/2	connected	desirable	channel	WS-C5505	066507453 (Sw 2/2
2/3	connected	desirable	channel	WS-C5505	066507453 (Sw 2/3
2/4	connected	desirable	channel	WS-C5505	066507453 (Sw 2/4

Ahora, si SwitchA sale por alguna razón, o si el nuevo hardware substituye SwitchA, SwitchB intenta restablecer el canal. Si el nuevo equipo no puede canalizar, SwitchB trata sus puertos 2/1-4 como puertos de NON-canalización normales. Éste es una de las ventajas del uso del **desirable mode**. Si el canal fue configurado con el PAgP en el modo y un lado de la conexión tiene un error de cierta clase o una restauración, puede causar a un estado de errDisable (apague) en el otro lado. Con el PAgP fijado en el desirable mode en cada lado, el canal estabiliza y renegocia la conexión EtherChannel.

[Enlace troncal y EtherChannel](#)

EtherChannel es independiente del enlace troncal. Puede activar el enlace troncal o puede dejar el enlace troncal desactivado. Usted puede también girar el enlace para todos los puertos antes de que usted cree el canal, o usted puede girarlo después de que usted cree el canal (como lo hacemos aquí). Por lo que el EtherChannel, no importa; el enlace y el EtherChannel son totalmente características diferentes. Lo relevante es que todos los puertos involucrados estén en el mismo modo: o son todo el enlace antes de que usted configure el canal o son todos no enlace antes de que usted configure el canal. Todos los puertos deben estar en el mismo estado de

troncal antes de que usted cree el canal. Una vez que se forma una canal, todo lo que se cambie en un puerto también se cambia para los otros puertos en el canal. Los módulos usados en esta plataforma de ensayo pueden hacer el enlace ISL o 802.1q. Por abandono, los módulos se fijan a los troncales automáticas y negocian el modo, así que significa que ellos trunk si el otro lado los pide al trunk, y ellos negocian si utilizar el método para la conexión troncal ISL o 802.1q. Si no pedido al trunk, trabajan como puertos normales del NON-enlace.

```
Switch-A (enable) show trunk 2
Port      Mode      Encapsulation  Status      Native vlan
-----
2/1      auto      negotiate      not-trunking  1
2/2      auto      negotiate      not-trunking  1
2/3      auto      negotiate      not-trunking  1
2/4      auto      negotiate      not-trunking  1
```

Existen diversas formas de activar los enlaces troncales. Por este ejemplo, fijamos SwitchA a deseable. El switch A ya está configurado para negociar. La combinación deseable/negocia las causas SwitchA para pedir SwitchB al trunk y para negociar el tipo de enlace para hacer (ISL o 802.1q). Puesto que SwitchB omite para autonegociar, SwitchB responde a la petición de SwitchA. Estos resultados ocurren:

```
Switch-A (enable) set trunk 2/1 desirable
Port(s) 2/1-4 trunk mode set to desirable.
Switch-A (enable)
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
1999 Dec 18 20:46:26 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
1999 Dec 18 20:46:28 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

```
Switch-A (enable) show trunk 2
Port      Mode      Encapsulation  Status      Native vlan
-----
2/1      desirable  n-isl          trunking    1
2/2      desirable  n-isl          trunking    1
2/3      desirable  n-isl          trunking    1
2/4      desirable  n-isl          trunking    1
```

El modo de enlace troncal se configuró como deseable. El resultado era que negociaron al modo de concentración links con el switch de vecino, y decidían sobre ISL (n-ISL). El estado actual es Enlace troncal. Esto es qué sucedió en SwitchB debido al comando publicado en SwitchA.

```
Switch-B (enable)
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 19:09:53 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
```

```

2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

```

```
Switch-B (enable) show trunk 2
```

Port	Mode	Encapsulation	Status	Native vlan
2/1	auto	n-isl	trunking	1
2/2	auto	n-isl	trunking	1
2/3	auto	n-isl	trunking	1
2/4	auto	n-isl	trunking	1

Note que los cuatro puertos (2/1-4) se convirtieron en trunks, aunque cambiamos solamente específicamente un puerto (2/1) a deseable. Éste es un ejemplo de cómo el cambio de un puerto en el canal afecta a todos los puertos.

Resolución de problemas de EtherChannel

Los desafíos para EtherChannel pueden dividirse en dos áreas principales: Troubleshooting dentro de la fase de configuración, y troubleshooting dentro de la fase de ejecución. Los errores de configuración ocurren, en general, debido a una discordancia de parámetros entre los puertos involucrados (velocidades distintas, dúplex distinto, valores de puerto del árbol de expansión distintos, etc.). Usted puede también generar los errores dentro de la configuración si usted fija el canal en un lado a **encendido** y la espera también mucho antes usted configura el canal en el otro lado. El causa los Spanning-Tree Loop, que genera un error, y apaga el puerto.

Cuando se encuentra un error mientras que usted configura el EtherChannel, esté seguro de marcar el estatus de los puertos después de que usted corrija la situación de error del EtherChannel. Si el estado del puerto es *errdisable*, ese significa que los puertos han sido apagados por el software y no se adelantan otra vez hasta que usted ingrese el **comando set port enable**.

Note: Si el estado del puerto hace *errdisable*, usted debe habilitar específicamente los puertos con el **comando set port enable** para que los puertos lleguen a ser activo. ¡Actualmente, usted puede corregir todos los problemas del EtherChannel pero los puertos no suben ni forman un canal hasta que se habiliten otra vez! Las versiones futuras del sistema operativo pueden marcar periódicamente si los *puertos ERRDISABLE* deben ser habilitados.

Para estas pruebas apagamos el enlace y el EtherChannel: Parámetros no coincidentes; Espera también mucho antes usted configura el otro lado; Estado de errDisable correcto; y demostración qué sucede cuando las interrupciones de link y se restablece.

Parámetros no coincidentes

Éste es un ejemplo de parámetros no coincidentes. El set port 2/4 en el VLAN2 mientras que los otros puertos todavía están en el VLA N 1. para crear un nuevo VLA N, nosotros debemos asignar un dominio VTP para el Switch y crear el VLA N.

```
Switch-A (enable) show port channel
No ports channelling
```

```
Switch-A (enable) show port
Port  Name          Status      Vlan      Level Duplex Speed Type
-----
2/1          connected  1         normal a-full a-100 10/100BaseTX
2/2          connected  1         normal a-full a-100 10/100BaseTX
2/3          connected  1         normal a-full a-100 10/100BaseTX
2/4          connected  1         normal a-full a-100 10/100BaseTX
```

```
Switch-A (enable) set vlan 2
Cannot add/modify VLANs on a VTP server without a domain name.
```

```
Switch-A (enable) set vtp domain testDomain
VTP domain testDomain modified
```

```
Switch-A (enable) set vlan 2 name vlan2
Vlan 2 configuration successful
```

```
Switch-A (enable) set vlan 2 2/4
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
-----
```

```
2      2/4
```

```
Switch-A (enable)
1999 Dec 19 00:19:34 %PAGP-5-PORTFROMSTP:Port 2/4 left bridg4
```

```
Switch-A (enable) show port
Port  Name          Status      Vlan      Level Duplex Speed Type
-----
2/1          connected  1         normal a-full a-100 10/100BaseTX
2/2          connected  1         normal a-full a-100 10/100BaseTX
2/3          connected  1         normal a-full a-100 10/100BaseTX
2/4          connected  2         normal a-full a-100 10/100BaseTX
```

```
Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.
```

```
Switch-A (enable)
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4
```

```
Switch-A (enable) show port channel
Port  Status      Channel  Channel  Neighbor  Neighbor
      mode       status   device   device    port
-----
2/1   connected  desirable channel   WS-C5505  066509957(Sw 2/1
2/2   connected  desirable channel   WS-C5505  066509957(Sw 2/2
-----
```

Note que el canal formó solamente entre los puertos 2/1-2. Los puertos 2/3-4 fueron salidos hacia fuera porque el puerto 2/4 estaba en un diverso VLA N. No había mensaje de error; PAgP sólo hizo lo que pudo para hacer funcionar el canal. Usted necesita mirar los resultados cuando usted crea el canal para asegurarse lo hizo lo que usted quisiera que hiciera.

Ahora fije el canal manualmente a encendido con el puerto 2/4 en un diverso vlan y vea qué sucede. Primero fijamos al modo del canal de nuevo al auto para derribar el canal actual, después fijamos el canal manualmente a encendido.

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
Switch-A (enable)
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:26:18 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4
```

```
Switch-A (enable) show port channel
No ports channelling
```

```
Switch-A (enable) set port channel 2/1-4 on
Mismatch in vlan number.
Failed to set port(s) 2/1-4 channel mode to on.
```

```
Switch-A (enable) show port channel
No ports channelling
```

En SwitchB podemos girar el canal y notar que dice la multa del canal de los puertos, pero sabemos que SwitchA no está configurado correctamente.

```
Switch-B (enable) show port channel
No ports channelling
```

```
Switch-B (enable) show port
Port  Name                Status      Vlan      Level Duplex Speed Type
-----
2/1                connected  1          normal a-full a-100 10/100BaseTX
2/2                connected  1          normal a-full a-100 10/100BaseTX
2/3                connected  1          normal a-full a-100 10/100BaseTX
2/4                connected  1          normal a-full a-100 10/100BaseTX
```

```
Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

```
Switch-B (enable)
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

```
Switch-B (enable) show port channel
Port  Status      Channel  Channel  Neighbor  Neighbor
-----
2/1  connected  on       channel  WS-C5505  066507453 (Sw 2/1
2/2  connected  on       channel  WS-C5505  066507453 (Sw 2/2
```

```

2/3 connected on channel WS-C5505 066507453 (Sw 2/3
2/4 connected on channel WS-C5505 066507453 (Sw 2/4
-----

```

Esto clarifica que usted debe los ambos lados de control del canal cuando usted configura manualmente el canal para asegurarse que los ambos lados están para arriba, no apenas un lado. Esta salida muestra que SwitchB está fijado para un canal, pero SwitchA no canaliza porque tiene un puerto que esté en el VLA N incorrecto.

Espera también mucho antes usted configura el otro lado

En nuestra situación, SwitchB tiene EtherChannel girado, pero SwitchA no hace porque tiene un Error de configuración vlan (los puertos 2/1-3 están en el vlan1, el puerto 2/4 están en vlan2). Aquí es qué sucede cuando un lado de un EtherChannel se fija a encendido mientras que el otro lado todavía está en el modo automático. SwitchB, después de algunos minutos, apaga sus puertos debido a una detección del loop que atravesaba. Esto se produce debido a que los puertos 2/1-4 del Switch B se comportan como si fueran un único puerto grande, mientras que los puertos 2/1-4 del Switch B son puertos totalmente independientes. Un broadcast enviado de SwitchB a SwitchA en el puerto 2/1 se devuelve a SwitchB en los puertos 2/2, 2/3 y 2/4 porque SwitchA trata estos puertos como puertos independientes. Es por ello que el SwitchB piensa que hay un loop de Spanning Tree. Note que los puertos en SwitchB ahora están inhabilitados y tenga un estatus del *errdisable*.

```

Switch-B (enable)
2000 Jan 17 22:55:48 %SPANTREE-2-CHNMISCFG: STP loop - channel 2/1-4 is disabled in vlan 1.
2000 Jan 17 22:55:49 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 22:56:01 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 22:56:13 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 22:56:36 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

```

```

Switch-B (enable) show port channel
Port Status Channel Channel Neighbor Neighbor
      mode status device port
-----
2/1 errdisable on channel
2/2 errdisable on channel
2/3 errdisable on channel
2/4 errdisable on channel
-----

```

```

Switch-B (enable) show port
Port Name Status Vlan Level Duplex Speed Type
-----
2/1 errdisable 1 normal auto auto 10/100BaseTX
2/2 errdisable 1 normal auto auto 10/100BaseTX
2/3 errdisable 1 normal auto auto 10/100BaseTX
2/4 errdisable 1 normal auto auto 10/100BaseTX

```

Corrija al estado de errDisable

A veces cuando usted intenta configurar el EtherChannel pero los puertos no se configuran lo mismo, causa los puertos en un lado del canal o el otro que se apagará. Las luces de link son amarillas en el puerto. Usted puede decir esto por la consola si usted teclea el **puerto de la demostración**. Los puertos se enumeran como *errdisable*. Para recuperarse de esto, usted debe reparar los parámetros unidos mal en los puertos implicados, después vuelve a permitir los puertos. Apenas observe eso para volver a permitir los puertos es un paso separado que se debe hacer para que los puertos lleguen a ser funcional otra vez.

En nuestro ejemplo sabemos que SwitchA tenía una discordancia vlan. Vamos a SwitchA e introducimos la parte posterior del puerto 2/4 al vlan1. Entonces giramos el canal para los puertos 2/1-4. SwitchA no muestra conectado hasta que volvamos a permitir los puertos de SwitchB. Entonces cuando hemos reparado SwitchA y lo pusimos en el modo de canalización, volvemos a SwitchB y volvemos a permitir los puertos.

```
Switch-A (enable) set vlan 1 2/4
VLAN 1 modified.
VLAN 2 modified.
VLAN Mod/Ports
```

```
-----
1      2/1-24
```

```
Switch-A (enable) set port channel 2/1-4 on
```

```
Port(s) 2/1-4 channel mode set to on.
```

```
Switch-A (enable) sh port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	notconnect	on	channel		
2/2	notconnect	on	channel		
2/3	notconnect	on	channel		
2/4	notconnect	on	channel		

```
Switch-B (enable) show port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	errdisable	on	channel		
2/2	errdisable	on	channel		
2/3	errdisable	on	channel		
2/4	errdisable	on	channel		

```
Switch-B (enable) set port enable 2/1-4
```

```
Ports 2/1-4 enabled.
```

```
Switch-B (enable) 2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridg4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

```
Switch-B (enable) show port channel
```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	on	channel		
2/2	connected	on	channel		
2/3	connected	on	channel		
2/4	connected	on	channel		

Demostración qué sucede cuando las interrupciones de link y se restablece

Cuando va un puerto en el canal abajo, cualquier paquete que se envíe normalmente en ese puerto se desplaza encima al puerto siguiente en el canal. Usted puede verificar esto sucede con el **comando show mac**. En nuestra plataforma de ensayo, hacemos que SwitchA envíe los paquetes ping a SwitchB para ver qué link utiliza el tráfico. Primero borramos los contadores,

después mostramos el mac, enviamos tres ping, y en seguida **mostramos el mac** otra vez para ver en qué canal fueron recibidas las respuestas al ping.

Switch-A (enable) **clear counters**

This command will reset all MAC and port counters reported in CLI and SNMP.

Do you want to continue (y/n) [n]? y

MAC and Port counters cleared.

Switch-A (enable) **show port channel**

Port	Status	Channel mode	Channel status	Neighbor device		Neighbor port
2/1	connected	on	channel	WS-C5505	066509957 (Sw	2/1
2/2	connected	on	channel	WS-C5505	066509957 (Sw	2/2
2/3	connected	on	channel	WS-C5505	066509957 (Sw	2/3
2/4	connected	on	channel	WS-C5505	066509957 (Sw	2/4

Switch-A (enable) **show mac**

Port	Rcv-Unicast	Rcv-Multicast	Rcv-Broadcast	
2/1		0	18	0
2/2		0	2	0
2/3		0	2	0
2/4		0	2	0

Switch-A (enable) **ping 172.16.84.17**

172.16.84.17 is alive

Switch-A (enable) **ping 172.16.84.17**

172.16.84.17 is alive

Switch-A (enable) **ping 172.16.84.17**

172.16.84.17 is alive

Switch-A (enable) **show mac**

Port	Rcv-Unicast	Rcv-Multicast	Rcv-Broadcast	
2/1		3	24	0
2/2		0	2	0
2/3		0	2	0
2/4		0	2	0

En este momento, hemos recibido las respuestas al ping en el puerto 3/1. Cuando la consola de SwitchB envía una respuesta a SwitchA, el EtherChannel utiliza el puerto 2/1. Ahora apagamos el puerto 2/1 en SwitchB. De SwitchA publicamos otro ping y vemos en qué canal se vuelve la respuesta. (SwitchA envía encendido el mismo puerto con el cual SwitchB está conectado. Sólo mostramos los paquetes recibidos del switch B porque los paquetes de transmisión aparecen más abajo en la pantalla show mac.)

1999 Dec 19 01:30:23 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

Switch-A (enable) **ping 172.16.84.17**

172.16.84.17 is alive

Switch-A (enable) **show mac**

Port	Rcv-Unicast	Rcv-Multicast	Rcv-Broadcast	
2/1		3	37	0
2/2		1	27	0
2/3		0	7	0

Ahora que se inhabilita el puerto 2/1, el EtherChannel utiliza automáticamente el puerto siguiente en el canal, 2/2. Ahora volvemos a permitir el puerto 2/1 y lo esperamos para unirnos a al Grupo de Bridge. Luego ejecutamos dos pings más.

```
1999 Dec 19 01:31:33 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
```

```
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac
```

Port	Rcv-Unicast	Rcv-Multicast	Rcv-Broadcast
2/1	5	50	0
2/2	1	49	0
2/3	0	12	0
2/4	0	12	0

Observe que estos ping están enviados del puerto 2/1. Cuando viene el link salvaguardia, el EtherChannel la agrega al conjunto y la utiliza otra vez. Todo esto se realiza en modo transparente para el usuario.

[Comandos utilizados en esta sección](#)

Éstos son los comandos que fueron utilizados en esta sección.

Comandos de utilizar para fijar la configuración

- **set port channel on** - girar la función EtherChannel.
- **set port channel auto** - reajustar los puertos a su modo automático predeterminado.
- **set port channel desirable** - enviar los paquetes PAGP al otro lado que pide que un canal esté creado.
- **permiso del set port** - habilitar los puertos después de la neutralización del set port o después de un estado de errDisable.
- **set port disable**: Para desactivar un puerto mientras se aplican otros valores de configuración.
- **set trunk desirable** - girar el enlace y hacer este puerto enviar una petición al otro Switch de indicar que esto es un link de troncal. Si el puerto se fija para negociar (la configuración predeterminada) para negociar el tipo de enlace para utilizar en el link (ISL o 802.1q).

Comandos de utilizar para verificar la configuración

- **versión de la demostración** - visualizar qué versión de software funciona con el Switch.
- **módulo show** - visualizar qué módulos están instalados en el Switch.
- **las capacidades de puerto de la demostración** - de determinar si los puertos que queremos utilizar tienen la capacidad de hacer el EtherChannel.
- **show port** - para determinar el estado del puerto (desconectado, conectado) y las configuraciones de dúplex y de velocidad.
- **ping** - probar la Conectividad al otro Switch.
- **show port channel** - Para ver el estado actual del agrupamiento de EtherChannel.

- **show port channel mod/port** - dar una más vista detallada del estado del canal de un puerto único.
- **show spantree** – para comprobar que el árbol de expansión detectó el canal como un link.
- **show trunk** - para ver el estado de conexión troncal de los puertos.

Comandos de utilizar para resolver problemas la configuración

- **show port channel** - Para ver el estado actual del agrupamiento de EtherChannel.
- **show port** - para determinar el estado del puerto (desconectado, conectado) y las configuraciones de dúplex y de velocidad.
- **clear counters** - para reiniciar los contadores de paquete del switch a cero. Los contadores se visualizan con el comando **show mac**.
- **mac de la demostración** - ver los paquetes recibidos y enviados por el Switch.
- **ping**: para comprobar la conectividad al otro switch y generar tráfico que aparezca con el comando **show mac**.

Utilización de Portfast y otros comandos para solucionar los problemas al iniciar la conectividad de la estación extremo

Si usted tiene puestos de trabajo conectados con el Switches que no pueden iniciar sesión a su dominio de red (NT o Novell), o no pueden conseguir un DHCP Address, después usted puede ser que quiera intentar las sugerencias enumeradas en este documento antes de que usted explore otras avenidas. Las sugerencias son relativamente fáciles de implementar y son muy a menudo la causa de los problemas de conectividad del puesto de trabajo encontrados durante la inicialización/la fase de inicio del puesto de trabajo.

Con cada vez más los clientes que despliegan la transferencia al escritorio y substituyen su Hubs compartido por el Switches, vemos a menudo los problemas introducidos en el cliente/los entornos de servidor debido a este retraso inicial. El problema principal que observamos es que Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Clientes y AppleTalk clientes no pueden conectarse con sus servidores. Si el software en estos dispositivos no es persistente dentro del procedimiento de inicialización abandonan intentar conectar con su servidor antes de que el Switch incluso haya permitido que el tráfico pase a través.

Note: Esta demora inicial en la conectividad a menudo se manifiesta como errores que aparecen cuando se inicia una estación de trabajo por primera vez. Éstos son varios ejemplos de los mensajes de error y de los errores que usted puede ver:

- Visualizaciones de un cliente de la interconexión de redes de Microsoft, “ningunos controladores de dominio disponibles.”
- Informes del DHCP, “ningunos servidores DHCP disponibles.”
- Una estación de trabajo de interconexión Novell IPX no muestra la pantalla "Novell Login Screen" al inicio.
- Se han interrumpido las visualizaciones de un cliente de las conexiones de red Appletalk, “acceso a su red Appletalk. Para restablecer su conexión, abierta y cerrar al panel de control AppleTalk.” Es también posible que la aplicación de selección del cliente del APPLE TALK o no visualiza una lista de zonas, o visualiza una lista de zonas incompleta.

El retardo de conectividad inicial también se observa con frecuencia en un entorno conmutado en el cual un administrador de red actualiza el software o los controladores. En este caso, un vendedor puede optimizar los drivers de modo que los procedimientos de inicialización de la red

sucedan anterior en el proceso de inicialización del cliente (antes de que el Switch está listo para procesar los paquetes).

Con las diversas características que ahora se incluyen en un poco de Switches, puede tomar cerca de un minuto para que un Switch comience a mantener un puesto de trabajo nuevamente conectado. Este retardo puede afectar al puesto de trabajo cada vez que se gira o se reinicia. Éstas son las cuatro funciones principales que causan este retardo:

- Spanning-Tree Protocol (STP)
- Negociación EtherChannel
- Negociación de enlaces troncales
- Negociación de velocidad de link/dúplex entre el switch y la estación de trabajo

Las cuatro características son mencionadas en orden de qué causa la mayoría del retardo (Spanning-Tree Protocol) al cual causa el menos retardo (negociación de dúplex/velocidad). Un puesto de trabajo conectado con un Switch no causa generalmente los Spanning-Tree Loop, no necesita generalmente el EtherChannel, y no necesita generalmente negociar un método de concentración de links. (Si usted inhabilita la velocidad/la negociación de la detección del link, puede también reducir el retardo de puerto si usted necesita optimizar su tiempo de inicio tanto cuanto sea posible.)

Esta sección muestra cómo implementar comandos de optimización de la velocidad de inicio en tres plataformas de switch Catalyst. En las secciones del temporizador, mostramos cómo se reduce la demora en el puerto del switch y en qué medida.

[Contenido](#)

1. [Antecedente](#)
2. [Cómo reducir el retardo de inicialización en el switch Catalyst 4000/5000/6000](#)
3. [Pruebas de sincronización en el Catalyst 5000](#)
4. [Cómo reducir el retardo de inicialización en el switch Catalyst 2900XL/3500XL](#)
5. [Pruebas de Timing en el Catalyst 2900XL](#)
6. [Cómo reducir el retardo de inicialización en el switch Catalyst 1900/2800](#)
7. [Prueba de sincronización en el Catalyst 2820](#)
8. [Beneficio adicional de Portfast](#)

Los términos “estación de trabajo”, “estación extrema”, “servidor” se utilizan indistintamente en esta sección. Qué referimos es cualquier dispositivo conectado directamente con un Switch por un solo indicador luminoso LED amarillo de la placa muestra gravedad menor NIC. Puede también referir a los dispositivos con las placas NIC múltiples donde el indicador luminoso LED amarillo de la placa muestra gravedad menor NIC se utiliza solamente para la Redundancia, es decir el puesto de trabajo o el servidor no se configura para actuar como Bridge, él apenas tiene placas NIC múltiples para la Redundancia.

Note: Existen algunas tarjetas NIC de servidor que soportan troncal y/o EtherChannel. Hay las situaciones donde el servidor necesita vivir en (el enlace) de varios VLA N al mismo tiempo o el servidor necesita más ancho de banda en el link que lo conecta con el Switch (EtherChannel). En estos casos usted no apaga el PAgP y usted no apaga el enlace. Asimismo, estos dispositivos rara vez se apagan o reinician. Las instrucciones que contiene este documento no se aplican a este tipo de dispositivos.

[Antecedente](#)

Esta sección cubre cuatro características que un poco de Switches tenga que los retrasos iniciales de la causa cuando un dispositivo está conectado con un Switch. Un puesto de trabajo no causa generalmente atravesar - problema del árbol (loops), ni necesita la característica (PAgP, DTP), así que el retardo es innecesario.

Spanning-tree

Si usted ha comenzado recientemente a trasladarse desde a entorno de hub a un entorno del Switch estos problemas de conectividad pueden aparecer porque un Switch funciona mucho diferentemente que un concentrador. Un Switch proporciona la Conectividad en la capa de transmisión de datos, no en la Capa física. El switch tiene que usar un algoritmo de conexión en puente para decidir si los paquetes recibidos en un puerto necesitan transmitirse a otros puertos. El algoritmo de conexión en puente es susceptible a loops físicos en la topología de red. Debido a esta susceptibilidad a los loops, el Switches funciona con un protocolo llamado el Spanning Tree Protocol (STP) ese los loops de las causas que se eliminarán en la topología. El funcionamiento del STP causa todos los puertos que se incluyan en atravesar - proceso del árbol a convertirse en mucho más lento activo que de otra manera, como detecta y bloquea los loops. Un Bridged Network que tiene loops físicos, sin atravesar - árbol, se rompe. A pesar del tiempo implicado, el STP es una buena cosa. El atravesar - el árbol que se ejecuta en los switches de Catalyst es una especificación del estándar de la industria (IEEE 802.1D).

Después de que un puerto en el Switch tenga link y se una a al Grupo de Bridge que ejecuta atravesar - árbol en ese puerto. El atravesar que se ejecuta del puerto - el árbol puede tener 1 de 5 estados: Bloqueo, escuchando, aprendiendo, remitiendo, y inhabilitado. El árbol de expansión indica que el puerto inicia el bloqueo y, luego, pasa rápidamente a las fases de escucha y aprendizaje. Por abandono pasa el aprendizaje segundos que escuchan y de los 15 de aproximadamente 15 segundos.

Mientras que en el estado de escucha, el Switch intenta determinar donde cabe en la topología del árbol de expansión. Quiere especialmente saber si este puerto es parte de al loop físico. Si es parte de al loop, este puerto se puede elegir para entrar el modo de bloqueo. El bloqueo significa que no envía ni que recibe los datos del usuario por la eliminación de los loops. Si el puerto no es parte de al loop, procede al estado de aprendizaje que implica el aprender de qué direcciones MAC viven apagado de este puerto. Todo este proceso de inicialización del árbol de expansión tarda alrededor de 30 segundos.

Si usted conecta un puesto de trabajo o un servidor con un solo indicador luminoso LED amarillo de la placa muestra gravedad menor NIC con un puerto del switch, esta conexión no puede crear un loop físico. Se considera que estas conexiones son nodos hoja. No hay razón para hacer esperar 30 segundos a la estación de trabajo mientras el switch verifica la presencia de loops cuando la estación de trabajo no puede provocar un loop. Cisco agregó tan una característica llamada "Portfast" o el "comienzo rápido", que significa atravesar - el árbol para este puerto asumirá que el puerto no es parte de al loop y se moverá inmediatamente al estado de reenvío, sin pasar con el bloqueo, escuchando, o los estados de aprendizaje. Esto puede ahorrar mucho tiempo. Este comando no desactiva el árbol de expansión. Simplemente, hace que el árbol de expansión en el puerto seleccionado saltee algunos pasos (innecesarios en este caso) al principio.

Note: La característica portfast se debe nunca utilizar en los puertos del switch que conectan con el otro Switches o Hubs o Routers. Estas conexiones pueden causar los loops físicos, y es muy importante que atravesando - el árbol pasa con el procedimiento de inicialización completo en estas situaciones. Un loop de spanning tree puede interrumpir el funcionamiento de su red. Si el portfast se gira para un puerto que sea parte de al loop físico, puede causar una ventana del

tiempo donde los paquetes podrían ser remitidos posiblemente continuamente (e incluso multiplicarse) de una manera tal que la red no pueda recuperarse. En más adelante software del sistema operativo Catalyst (5.4(1)), hay una característica llamada el protector Portfast BPDU, que detecta la recepción de los BPDU en los puertos que tienen Portfast habilitaron. Puesto que esto debe nunca suceder, la Protección BPDU pone el puerto en el estado del "errdisable".

EtherChannel

Otros ofrecen un Switch pueden tener se llaman EtherChannel (o Fast EtherChannel, o Gigabit EtherChannel). Esta característica permite que los links múltiples entre los mismos dos dispositivos trabajen como si fueran un link rápido, con la carga de tráfico equilibrada entre los links. Un Switch puede formar a estos conjuntos automáticamente con un vecino con un protocolo llamado Port Aggregation Protocol (PAgP). Los puertos del switch que pueden ejecutar el valor por defecto del PAgP generalmente a un modo pasivo llamaron el "auto" que significa que él puede formar a un conjunto si el dispositivo vecino a través del link lo pide a. Si usted funciona con el protocolo en el modo automático, puede hacer un puerto retrasar para hasta 15 segundos antes de que pasa el control al algoritmo del árbol de expansión (el PAgP se ejecuta en un puerto antes de atravesar - el árbol hace). No hay razón del PAgP para ejecutarse en un puerto conectado con un puesto de trabajo. Si usted fija al modo PAgP del puerto del switch a "apagado," elimina este retardo.

Trunking

Otra característica del switch es la capacidad que posee un puerto de formar una troncal. Cuando se necesita transportar el tráfico desde las Redes virtuales de área local (VLAN), se configura un tronco entre dos dispositivos. UN VLA N es algo conmuta crea para hacer que un grupo de los puestos de trabajo aparece ser en sus los propio "segmento" o "dominio de broadcast." Los puertos troncales hacen que estas VLAN se extiendan por múltiples switches, de modo que una única VLAN pueda cubrir una oficina central completa. Hacen esto con la adición de las etiquetas a los paquetes; esto indica a qué VLA N pertenece el paquete.

Existen diversos tipos de protocolos trunking. Si un puerto puede convertirse en un trunk, puede también tener la capacidad al trunk automáticamente, y en algunos casos incluso negocia qué tipo de enlace a utilizar en el puerto. Esta capacidad de negociar el método de conexión troncal con el otro dispositivo se denomina Protocolo de concentración de enlaces dinámico (DTP), cuyo precursor es un protocolo denominado ISL dinámico (DISL). Si estos protocolos se ejecutan pueden retardar un puerto en el switch que se activa.

En general, un puerto conectado con una estación de trabajo pertenece a una sola VLAN y, en consecuencia, no necesita conectarse mediante un enlace troncal. Si un puerto tiene la capacidad de negociar la formación de un trunk omite generalmente el modo "auto". Si el puerto se cambia a un modo de concentración links de "OFF" reduce más lejos el retardo de un puerto del switch que llega a ser activo.

Negociación de velocidad y dúplex

Por lo general, alcanza con encender el Portfast y apagar el PAgP (si está presente) para resolver el problema, pero si necesita eliminar cada segundo posible puede también configurar la velocidad del puerto y realizar un dúplex manualmente sobre el switch si se trata de un puerto de velocidades múltiples (10/100). La negociación automática es una buena característica pero el torneado de ella apagado podría salvarle 2 segundos en un Catalyst 5000 (no ayuda a mucho en los 2800 o el 2900XL).

Puede haber complicaciones, sin embargo, si apaga la negociación automática en el switch pero la deja activa en la estación de trabajo. Puesto que el Switch no negocia con el cliente, el cliente no pudo elegir la misma configuración dúplex que el Switch utiliza. Vea “la mitad/la negociación automática del dúplex completo y del semidúplex de los Ethernetes 10/100Mb del troubleshooting” para más información sobre las advertencias de la negociación automática.

[Cómo reducir el retardo de inicialización en el switch Catalyst 4000/5000/6000](#)

Estos cinco comandos show cómo girar Portfast, cómo apagar la negociación PAgP, apagan la negociación de links (DISL, DTP) y apagan la negociación de dúplex/velocidad. El **portfastcommand del spantree del conjunto** se puede hacer en un rango de puertos inmediatamente (**fije el permiso del spantree PortFast 2/1-12**). El **canal del set port** se debe apagar generalmente con un grupo válido de puertos aptos para canal. En este caso el módulo dos tiene la capacidad de canalizar con los puertos 2/1-2 o con los puertos 2/1-4, así que cualquiera de estos grupos de puertos habría sido válido utilizar.

Note: La versión 5.2 del Cat OS para el Catalyst 4000/5000 tiene un comando new llamado el **host del set port** que es una macro que combina estos comandos en un comando fácil de usar (a menos que no cambia las configuraciones de la velocidad y dúplex).

Configuración

```
Switch-A (enable) set spantree portfast 2/1 enable
```

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.

```
Spantree port 2/1 fast start enabled.
```

```
Switch-A (enable) set port channel 2/1-2 off
```

```
Port(s) 2/1-2 channel mode set to off.
```

```
Switch-A (enable) set trunk 2/1 off
```

```
Port(s) 2/1 trunk mode set to off.
```

Los cambios en la configuración se guardan automáticamente en NVRAM.

Verificación

La versión de software de switch que se utiliza en este documento es 4.5(1). Para el resultado completo de la versión y del módulo show de la demostración refiera a esta sección de prueba de sincronización.

```
Switch-A (enable) show version
```

```
WS-C5505 Software,
```

```
Version McpSW: 4.5(1) NmpSW: 4.5(1)
```

Este comando muestra cómo ver al estado actual de un puerto en lo que respecta a atravesar - árbol. El puerto consiste actualmente en atravesar - el estado de reenvío del árbol (que envía y que recibe los paquetes) y la columna del comienzo rápido muestra que el portfast está inhabilitado actualmente. En otras palabras, el puerto tardará al menos 30 segundos en mudarse al estado de reenvío al iniciarse.

```
Switch-A (enable) show port spantree 2/1
```

Port	Vlan	Port-State	Cost	Priority	Fast-Start	Group-Method
2/1	1	forwarding	19	32		

disabled

Ahora habilitamos el portfast en este puerto del switch. El Switch nos advierte que este comando se deba utilizar solamente en los puertos que están conectados con un solo host (un puesto de trabajo, un servidor, un etc.) y nunca utilizar en los puertos conectados con el otro Hubs o Switches. La razón que permitimos al portfast es así que el comienzo del puerto para remitir inmediatamente. ¿Podemos hacer esto porque un puesto de trabajo o un servidor no causa un loop de la red, así que porqué el marcar del tiempo de la basura? Pero otro hub o switch puede causar un loop, y queremos pasar siempre a través de las etapas de escucha y aprendizaje normales cuando conectamos con estos tipos de dispositivos.

```
Switch-A (enable) set spantree portfast 2/1 enable
```

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.

```
Spantree port 2/1 fast start enabled.
```

Para verificar que Portfast esté habilitado para este puerto haga este comando.

```
Switch-A (enable) show port spantree 2/1
```

Port	Vlan	Port-State	Cost	Priority	Fast-Start	Group-Method
2/1	1	forwarding	19	32		

enabled

Otra forma de visualizar la configuración de Portfast para un puerto, o más de uno, es ver la información del árbol de expansión para una VLAN determinada. Más tarde en la sección del temporizador de este documento, mostramos cómo hacer que el Switch señale cada etapa de atravesar - el árbol que mueve a través en el tiempo real. Esta salida también muestra el tiempo de retardo de reenvío (15 segundos). Este es el tiempo que permanecerá el árbol de expansión en el estado de escucha y el que permanecerá en el estado de aprendizaje por cada puerto de la VLAN.

```
Switch-A (enable) show spantree 1
```

VLAN 1

```
Spanning tree enabled
```

```
Spanning tree type          ieee
```

```
Designated Root             00-e0-4f-94-b5-00
```

```
Designated Root Priority    8189
```

```
Designated Root Cost       19
```

```
Designated Root Port       2/24
```

```
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec
```

```
Bridge ID MAC ADDR         00-90-92-b0-84-00
```

```
Bridge ID Priority         32768
```

Bridge Max Age 20 sec Hello Time 2 sec **Forward Delay 15 sec**

Port	Vlan	Port-State	Cost	Priority	Fast-Start	Group-Method
2/1	1	forwarding	19	32	enabled	
...						

Para verificar que PAgP esté desactivado, utilice el comando **show port channel** . Esté seguro y especifique el número de módulo (2 en este caso) de modo que el comando le muestre el modo del canal incluso si no hay canal formado. Si **mostramos el Canal de puerto** sin los canales formados, apenas no dice ninguna canalización de los puertos. Deseamos avanzar y ver el modo de canal actual.

```
Switch-A (enable) show port channel  
No ports channeling
```

```
Switch-A (enable) show port channel 2  
Port Status Channel Channel Neighbor Neighbor  
----- mode status device port  
-----  
2/1 notconnect auto not channel  
2/2 notconnect auto not channel  
...
```

```
Switch-A (enable) set port channel 2/1-2 off  
Port(s) 2/1-2 channel mode set to off.
```

```
Switch-A (enable) show port channel 2  
Port Status Channel Channel Neighbor Neighbor  
----- mode status device port  
-----  
2/1 connected off not channel  
2/2 connected off not channel  
...
```

Para verificar que la negociación de links esté apagada, utilice el **comando set trunk off**. Mostramos el estado predeterminado. Luego, desactivamos la concentración de enlaces. Luego, mostramos el estado resultante. Especificamos el número 2 de módulo para que podamos ver el modo del canal actual para los puertos en este módulo.

```
Switch-A (enable) show trunk 2  
Port Mode Encapsulation Status Native vlan  
-----  
2/1 auto negotiate not-trunking 1  
2/2 auto negotiate not-trunking 1  
...
```

```
Switch-A (enable) set trunk 2/1-2 off  
Port(s) 2/1-2 trunk mode set to off.
```

```
Switch-A (enable) show trunk 2  
Port Mode Encapsulation Status Native vlan  
-----  
2/1 off negotiate not-trunking 1  
2/2 off negotiate not-trunking 1
```

No debe ser necesario excepto en el más raro de los casos apagar la negociación automática de

dúplex/velocidad o fijar manualmente la velocidad y dúplex en el Switch. Damos un ejemplo de cómo hacer esto en las pruebas de temporización con y sin el DTP, PAgP, y Portfast en una sección del Catalyst 5000 si usted la siente es necesario para su situación.

[Pruebas de sincronización con y sin DTP, PagP y PortFast en Catalyst 5000](#)

Esta prueba muestra qué sucede con la sincronización de inicialización del puerto del switch mientras que los diversos comandos son aplicados. Las configuraciones predeterminadas del puerto se usan en primer lugar para dar una referencia. Hacen el portfast inhabilitar, fijan al modo de PAgP (EtherChannel) al auto (canaliza si está pedido canalizar), y fijan al modo de concentración links (DTP) al auto (él los trunks si está pedido al trunk). La prueba entonces procede al portfast de la vuelta encendido y mide el tiempo, después da vuelta al PAgP a apagado y mide el tiempo, después apaga el enlace y mide el tiempo. Finalmente, desactivamos la negociación automática y medimos el tiempo. Todas estas pruebas se hacen en un Catalyst 5000 con un indicador luminoso LED amarillo de la placa muestra gravedad menor de los fast ethernet de 10/100 que soporte el DTP y el PAgP.

Note: El portfast de torneado prendido no está la misma cosa que dando vuelta a atravesar - árbol apagado (como se apunta en el documento). Con el portfast encendido, atravesando - el árbol todavía se ejecuta en el puerto; apenas no bloquea, escucha, o aprende, y va inmediatamente al estado de reenvío. Dando vuelta a atravesar - el árbol apagado no se recomienda porque afecta al VLA N entero y puede dejar la red vulnerable a los loops de la topología física, que pueden causar los problemas de red grave.

1. Muestre la versión del IOS del switch y la configuración (show version, show module).

```
Switch-A (enable) show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0 Model: WS-C5505 Serial #: 066507453

Mod Port Model Serial # Versions
-----
1 0 WS-X5530 006841805 Hw : 1.3
Fw : 3.1.2
Fw1: 3.1(2)
Sw : 4.5(1)
2 24 WS-X5225R 012785227 Hw : 3.2
Fw : 4.3(1)
Sw : 4.5(1)

          DRAM          FLASH          NVRAM
Module Total Used Free Total Used Free Total Used Free
-----
1 32640K 13648K 18992K 8192K 4118K 4074K 512K 119K 393K

Uptime is 28 days, 18 hours, 54 minutes

Switch-A (enable) show module
Mod Module-Name Ports Module-Type Model Serial-Num Status
-----
1 0 Supervisor III WS-X5530 006841805 ok
2 24 10/100BaseTX Ethernet WS-X5225R 012785227 ok
```



```

Mod MAC-Address(es)                               Hw      Fw      Sw
-----
1  00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2   4.5(1)
2  00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)  4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1  NFFC      WS-F5521  0008728786 1.0

```

2. Fije el registro para atravesar - árbol al más prolijo (fije el spantree del nivel de registro 7).
 Éste es el nivel de registro predeterminado (2) para atravesar - el árbol, así que significa que
 solamente las situaciones críticas están señaladas.

```

Switch-A (enable) show version
WS-C5505 Software, Version McpsW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0  Model: WS-C5505  Serial #: 066507453

```

```

Mod Port Model      Serial #  Versions
-----
1  0      WS-X5530  006841805 Hw : 1.3
                                   Fw : 3.1.2
                                   Fw1: 3.1(2)
                                   Sw : 4.5(1)
2  24     WS-X5225R 012785227 Hw : 3.2
                                   Fw : 4.3(1)
                                   Sw : 4.5(1)

```

```

          DRAM          FLASH          NVRAM
Module Total  Used   Free   Total  Used   Free   Total Used  Free
-----
1          32640K 13648K 18992K  8192K  4118K  4074K  512K 119K 393K

```

Uptime is 28 days, 18 hours, 54 minutes

```

Switch-A (enable) show module
Mod Module-Name      Ports Module-Type      Model      Serial-Num Status
-----
1                   0      Supervisor III    WS-X5530  006841805 ok
2                   24     10/100BaseTX Ethernet WS-X5225R 012785227 ok

```

```

Mod MAC-Address(es)                               Hw      Fw      Sw
-----
1  00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2   4.5(1)
2  00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)  4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1  NFFC      WS-F5521  0008728786 1.0

```

El nivel para atravesar - el árbol se cambia a 7 (debug), así que podemos ver el cambio de estados del árbol de expansión en el puerto. Este cambio de configuración sólo dura para la sesión terminal, luego vuelve a la normalidad.

```

Switch-A (enable) set logging level spantree 7
System logging facility <spantree for this session set to severity 7(debugging)

```

```
Switch-A (enable) show logging
...

Facility           Default Severity      Current Session Severity
-----
...
spanntree          2                      7
...
```

3. Comenzar con el puerto ubicado en el cierre del Catalyst.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

4. Ahora el tiempo y habilita el puerto. Deseamos saber por cuánto tiempo permanece en cada estado.

```
Switch-A (enable) show time
Fri Feb 25 2000, 12:20:17
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 12:20:39 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 12:20:39 %SPANTREE-6-PORTBLK: port 2/1 state in vlan 1 changed to blocking.
2000 Feb 25 12:20:39 %SPANTREE-6-PORTLISTEN: port 2/1 state in vlane 1 changed to
Listening.
2000 Feb 25 12:20:53 %SPANTREE-6-PORTLEARN: port 2/1 state in vlan 1 changed to Learning.
2000 Feb 25 12:21:08 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Aviso de la salida que tardó cerca de 22 segundos (20:17 a 20:39) para que el puerto comience la etapa del bloqueo del árbol de expansión. Éste era el tiempo que tomó para negociar el link y para hacer las tareas DTP y del PAgP. Cuando el bloqueo comienza, ahora consistimos en atravesar - reino del árbol. De bloquear el puerto, fue inmediatamente a escuchar (20:39 a 20:39). El paso desde escuchar a aprender insumió aproximadamente 14 segundos (20:39 a 20:53). Desde aprendizaje a reenvío tardó 15 segundos (de 20:53 a 21:08). Por lo tanto, el tiempo total antes de que el puerto entre en actividad para el tráfico, fue de aproximadamente 51 segundos (de 20:17 a 21:08). **Note:** Técnicamente, las etapas de escucha y de aprendizaje deben ser ambas de 15 segundos, que es como se establece el parámetro de retardo de reenvío para esta VLAN. La etapa de aprendizaje es probablemente más cercano a 15 segundos que 14 segundos si teníamos más mediciones precisas. Ninguna de las medidas que aquí se detallan son perfectamente precisas.

Acabamos de intentar dar una toma de las cosas de la sensación durante cuánto tiempo.

5. Sabemos de la salida y del comando **show spantree** que atravesando - el árbol es activo en este puerto. Miremos otras cosas que podrían reducir el puerto mientras que alcanza al estado de reenvío. El comando **show port capabilities** muestra que este puerto tiene la capacidad para implementar enlaces troncales y crear un EtherChannel. El comando **show trunk** muestra que este puerto está en modo automático y que está configurado para negociar el tipo de conexión troncal a utilizar (ISL o 802.1q, negociado a través del Protocolo troncal dinámico (DTP)).

```
Switch-A (enable) show port capabilities 2/1
Model                WS-X5225R
Port                 2/1
Type                 10/100BaseTX

Speed                auto,10,100
Duplex               half,full
```

```

Trunk encap type      802.1Q, ISL
Trunk mode          on, off, desirable, auto, nonegotiate
Channel            2/1-2, 2/1-4
Broadcast suppression percentage(0-100)
Flow control          receive-(off, on), send-(off, on)
Security              yes
Membership            static, dynamic
Fast start            yes
Rewrite               yes
Switch-A (enable) show trunk 2/1
Port      Mode      Encapsulation  Status      Native vlan
-----  -
2/1      auto      negotiate    not-trunking  1

```

6. Primero, habilitaremos Portfast en el puerto. La negociación de links (DTP) todavía está en el modo automático, y el EtherChannel (PAgP) todavía está en el modo automático.

```

Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

```

```

Switch-A (enable) set spantree portfast 2/1 enable

```

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.

```

Spantree port 2/1 fast start enabled.

```

```

Switch-A (enable) show time

```

```

Fri Feb 25 2000, 13:45:23

```

```

Switch-A (enable) set port enable 2/1

```

```

Port 2/1 enabled.

```

```

Switch-A (enable)

```

```

Switch-A (enable)

```

```

2000 Feb 25 13:45:43 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1

```

```

2000 Feb 25 13:45:44 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change to forwarding.

```

¡Ahora tenemos un tiempo total de 21 segundos! Transcurren 20 segundos antes de que se una al grupo puente (45:23 a 45:43). Pero después, una vez habilitado Portfast, STP comienza a reenviar en sólo un segundo (en lugar de 30 segundos). Al habilitar PortFast ahorramos 29 segundos. Veamos si podemos reducir aún más el retraso.

7. Ahora damos vuelta al modo PAgP a "apagado." Podemos ver del comando show port channel que fijan al modo PAgP al *auto*, que significa que canaliza si es pedido por a un vecino que hable el PAgP. Debe desactivar los canales para al menos un grupo de dos puertos. No puede hacerlo para un solo puerto.

```

Switch-A (enable) show port channel 2/1

```

```

Port  Status      Channel  Channel  Neighbor  Neighbor
      mode          status   device   port
-----  -
2/1   connected  auto    not channel

```

```

Switch-A (enable) set port channel 2/1-2 off

```

```

Port(s) 2/1-2 channel mode set to off.

```

8. Apague el puerto y repita la prueba.

```

Switch-A (enable) set port disable 2/1

```

```

Port 2/1 disabled.

```

```

Switch-A (enable) show time

```

```

Fri Feb 25 2000, 13:56:23

```

```
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 13:56:32 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:56:32 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Como se indicó anteriormente ahora sólo insume 9 segundos alcanzar el estado de reenvío (56:23 a 56:32) en lugar de 21 segundos, como sucedía con la prueba anterior. El PAgP de torneado del *auto* a *apagado* en esta prueba guardó cerca de 12 segundos.

9. Dé vuelta al enlace a apagado (en vez del auto) y vea cómo ese afecta al tiempo que toma para que el puerto alcance al estado de reenvío. Damos vuelta otra vez al puerto de vez en cuando, y registramos el tiempo.

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Iniciar la prueba con el troncal desactivado (en lugar de auto).

```
Switch-A (enable) show time
Fri Feb 25 2000, 14:00:19
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 14:00:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 14:00:23 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change for forwarding.
```

Ahorramos algunos segundos al comienzo dado que sólo llevó 4 segundos alcanzar el estado de reenvío del árbol de expansión (00:19 a 00:22). Guardamos cerca de 5 segundos cambiando al modo de concentración links del *auto* a *apagado*.

10. (Opcional) si la hora de inicialización del puerto del switch era el problema debe ser solucionada ahora. Si usted tiene que afeitar algunos más segundos del tiempo, usted podría fijar el puerto la velocidad y dúplex manualmente en vez de usar el autonegotiation. Si usted fija la velocidad y dúplex manualmente en nuestro lado, requiere que usted fije la velocidad y dúplex en el otro lado, también. Esto es porque fija la velocidad de puerto y la negociación automática de las neutralizaciones del duplex en el puerto, y el dispositivo de conexión no ve los parámetros de negociación automática. El dispositivo de conexión conecta solamente en semidúplex y los resultados de la discordancia dúplex del resultado en el rendimiento pobre y los errores de puerto. Recuerde que si configura la velocidad y el dúplex de un lado, debe hacer lo mismo en el dispositivo de conexión para evitar estos problemas. Para ver el estado del puerto después de fijar la velocidad y dúplex **muestre el puerto**.

```
Switch-A (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Switch-A (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Switch-A (enable) show port
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1		connected	1	normal	full	100	10/100BaseTX
...							

Éstos son los resultados de la sincronización:

```
Switch-A (enable) show time
Fri Feb 25 2000, 140528 Eastern
Switch-A (enable) set port enable 2/1
```

```
Port 2/1 enabled.  
Switch-A (enable)  
2000 Feb 25 140529 Eastern -0500 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1  
2000 Feb 25 140530 Eastern -0500 %SPANNTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to  
forwarding.
```

El resultado final da un tiempo de 2 segundos (0528 a 0530).

11. Hicimos otra visualmente prueba controlada por reloj (miramos nuestros relojes) comenzando un ping continuo (ping - t) dirigido al Switch en un PC asociado al Switch. Luego, desconectamos el cable del switch. Los ping comenzaron a fallar. Luego volvimos a conectar el cable al switch y observamos nuestros relojes para ver cuánto demoraba el switch en responder a los pings de la PC. Tomó alrededor de 5-6 segundos para que se encendiera la negociación automática para velocidad y dúplex y alrededor de 4 segundos para que apagara la negociación automática para velocidad y dúplex. Hay muchas variables en esta prueba (inicialización PC, software PC, puerto de la consola del Switch que responde a las peticiones, etc.), pero acabamos de querer conseguir una cierta sensación durante cuánto tiempo tomaría para conseguir una respuesta del punto de vista PC. Todas las pruebas eran desde el punto de vista interno del mensaje del debug del Switches.

[Cómo reducir el retardo de inicialización en el switch Catalyst 2900XL/3500XL](#)

Los modelos 2900XL y 3500XL se pueden configurar de un buscador Web, o por el SNMP, o por el comando line interface(cli). Utilizamos el CLI. Esto es un ejemplo donde vemos al estado del árbol de expansión de un puerto, gira el portfast, y después lo verifica que está prendido. El 2900XL/3500XL soporta el EtherChannel y el enlace, pero no soporta la creación dinámica del EtherChannel (PAgP) o la negociación del tronco dinámico (DTP) en la versión que probamos (11.2(8.2)SA6), así que no tenemos ninguna necesidad de darles vuelta apagado en esta prueba. También, después de que giremos el portfast, el tiempo transcurrido para que el puerto suba es ya menos de 1 segundo, tan allí no es mucha punta a intentar cambiar las configuraciones de la negociación de dúplex/velocidad para acelerar las cosas. Esperamos que un segundo sea lo suficientemente rápido. Por abandono, el portfast está apagado en los puertos del switch. Éstos son los comandos de girar el portfast:

Configuración

```
2900XL#conf t  
2900XL(config)#interface fastEthernet 0/1  
2900XL(config-if)#spanning-tree portfast  
2900XL(config-if)#exit  
2900XL(config)#exit  
2900XL#copy run start
```

Esta plataforma es como el IOS del router; usted debe salvar la configuración (**comienzo del funcionamiento de copia**) si usted quisiera que fuera guardada permanentemente.

Verificación

Para verificar que Portfast esté habilitado, haga este comando:

```
2900XL#show spanning-tree interface fastEthernet 0/1  
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
```

```
Port path cost 19, Port priority 128
Designated root has priority 8192, address 0010.0db1.7800
Designated bridge has priority 32768, address 0050.8039.ec40
Designated port is 13, path cost 19
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 2105, received 1
The port is in the portfast mode
```

Mire la configuración del switch.

```
2900XL#show running-config
Building configuration...

Current configuration:
!
version 11.2
...
!
interface VLAN1
 ip address 172.16.84.5 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
!
...
```

[Pruebas de Timing en el Catalyst 2900XL](#)

Éstas son las pruebas de temporización en el Catalyst 2900XL.

1. La versión de software 11.2(8.2)SA6 fue utilizada en el 2900XL para estas pruebas.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 11.2(8.2)SA6, MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Jun-99 16:25 by boba
Image text-base: 0x00003000, data-base: 0x00259AEC

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 week, 4 days, 22 hours, 5 minutes
System restarted by power-on
System image file is "flash:c2900XL-c3h2s-mz-112.8.2-SA6.bin", booted via console

cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes of
memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
```

Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF

2. Quisiéramos que el Switch nos dijera qué sucede y cuando sucede, así que ingresamos estos comandos:

```
2900XL(config)#service timestamps debug uptime
2900XL(config)#service timestamps log uptime
2900XL#debug spanntree events
Spanning Tree event debugging is on
2900XL#show debug
General spanning tree:
  Spanning Tree event debugging is on
```

3. Luego, cerramos el puerto en cuestión.

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#shut
2900XL(config-if)#
00:31:28: ST: sent Topology Change Notice on FastEthernet0/6
00:31:28: ST: FastEthernet0/1 - blocking
00:31:28: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
00:31:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

4. En este momento pegamos estos comandos del tablero en el Switch. Estos comandos muestran el tiempo en el 2900XL y reactiva el puerto:

```
show clock
conf t
int f0/1
no shut
```

5. Por defecto, Portfast está desactivado. Puede confirmarlo de dos formas. La primera manera es que el comando **show spanning-tree interface** no menciona Portfast. La segunda manera es mirar los config corrientes donde usted no ve el comando **spanning-tree portfast** bajo interfaz.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
  Port path cost 19, Port priority 128
  Designated root has priority 8192, address 0010.0db1.7800
  Designated bridge has priority 32768, address 0050.8039.ec40
  Designated port is 13, path cost 19
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 887, received 1
[Note: there is no message about being in portfast mode is in this spot...]
```

```
2900XL#show running-config
Building configuration...
...
```

```
!  
interface FastEthernet0/1  
[Note: there is no spanning-tree portfast command under this interface...]  
!
```

6. Aquí está la primera prueba de temporización con Portfast desconectado.

```
2900XL#show clock  
*00:27:27.632 UTC Mon Mar 1 1993  
2900XL#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
2900XL(config)#int f0/1  
2900XL(config-if)#no shut  
2900XL(config-if)#  
00:27:27: ST: FastEthernet0/1 - listening  
00:27:27: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up  
00:27:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to  
up  
00:27:42: ST: FastEthernet0/1 - learning  
00:27:57: ST: sent Topology Change Notice on FastEthernet0/6  
00:27:57: ST: FastEthernet0/1 - forwarding
```

El tiempo total de apaga hasta que el envío comenzado puerto fuera **30 segundos (27:27 a 27:57)**

7. Para girar Portfast, haga esto:

```
2900XL#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
2900XL(config)#interface fastEthernet 0/1  
2900XL(config-if)#spanning-tree portfast  
2900XL(config-if)#exit  
2900XL(config)#exit  
2900XL#
```

Para verificar que Portfast esté habilitado, utilice el comando **show spanning-tree interface**. Observe que el resultado del comando (casi al final) indica que Portfast está habilitado.

```
2900XL#show spanning-tree interface fastEthernet 0/1  
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING  
  Port path cost 19, Port priority 128  
  Designated root has priority 8192, address 0010.0db1.7800  
  Designated bridge has priority 32768, address 0050.8039.ec40  
  Designated port is 13, path cost 19  
  Timers: message age 0, forward delay 0, hold 0  
  BPDU: sent 1001, received 1
```

The port is in the portfast mode

También puede observar que Portfast se activa en la salida de configuración.

```
2900XL#sh ru  
Building configuration...  
...  
interface FastEthernet0/1  
  spanning-tree portfast  
...  
...
```

8. Ahora haga la prueba de temporización con Portfast habilitó

```
2900XL#show clock  
*00:23:45.139 UTC Mon Mar 1 1993
```



```

2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:23:45: ST: FastEthernet0/1 -jump to forwarding from blocking
00:23:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:23:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

```

En este caso, el tiempo total era inferior a 1 segundo. Si el retardo de la inicialización de puerto en el Switch era el problema, el portfast debe solucionarlo. Recuerde, el switch no admite actualmente la negociación troncal, por lo que no es necesario desactivarla. Ni soporta el PAgP para el enlace, así que no necesitamos apagarlo, cualquiera. El switch admite la negociación automática de velocidad y dúplex. Sin embargo, dado que el retraso es tan pequeño, no es necesario desconectarlo.

9. También hicimos la prueba de ping de un puesto de trabajo al Switch. La respuesta tardó 5 a 6 segundos en llegar desde el switch, sin importar si la negociación automática de velocidad y dúplex estaba activada o desactivada.

[Cómo reducir el retardo de inicialización en el switch Catalyst 1900/2800](#)

El 1900/2820 refiere a Portfast por otro nombre: Principio-expedición de Spantree. Para la versión de software nos ejecutamos (V8.01.05), el valor por defecto del Switches a esto: Portfast se habilita en los puertos de los Ethernetes (10Mbps), y Portfast se inhabilita en los puertos de los fast ethernet (uplink). Así pues, cuando usted **muestra el funcionamiento** para ver la configuración, si un acceso de Ethernet no dice nada sobre Portfast, después se habilita Portfast. Si no dice "ninguna principio-expedición del spantree" en la configuración, se inhabilita Portfast. En un puerto del FastEthernet (100Mbps), el contrario es verdad: Para un puerto FastEthernet, Portfast está conectado sólo si el puerto muestra "spantree start-forwarding" en la configuración.

Aquí hay un ejemplo de cómo configurar Portfast en un puerto FastEthernet. Estos ejemplos utilizan la versión 8 de Enterprise edition software (Software de edición para empresas). El 1900 guarda automáticamente la configuración después de que se hayan realizado los cambios. Recuerde, usted no querría Portfast habilitado en cualquier puerto que conecte con otro Switch o concentrador, sólo si el puerto asocia a una estación final. La configuración se guarda automáticamente en NVRAM.

Configuración

```

1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.05
Copyright (c) Cisco Systems, Inc. 1993-1998
1900 uptime is 0day(s) 01hour(s) 10minute(s) 42second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-50-E1-A4-80
1900#conf t
Enter configuration commands, one per line.  End with CNTL/Z

```

```
1900(config)#interface FastEthernet 0/26
1900(config-if)#spanntree start-forwarding
1900(config-if)#exit
1900(config)#exit
1900#
```

Verificación

Una forma de verificar si PortFast está activado es consultando la configuración. Recuerde que un puerto FastEthernet debe decir que está prendido. La tiene un puerto Ethernet salvo que la configuración muestre que está desactivada. En esta configuración, la interfaz Ethernet 0/1 tiene portfast apagado (usted puede ver el comando de apagarlo), las interfaces Ethernet 0/2 tiene portfast encendido (usted no ve nada - que significa que está prendido), y el FastEthernet 0/26 de la interfaz (vire A hacia el lado de babor en el sistema de menús) tiene portfast encendido (usted puede ver el comando de girarlo).

```
1900#show running-config
Building configuration...
...
!
interface Ethernet 0/1

    no spanntree start-forwarding
!
interface Ethernet 0/2

!
...
!
interface FastEthernet 0/26
    spanntree start-forwarding
```

La forma más sencilla de visualizar el estado portfast es a través del sistema de menú. Si usted elige (p) para la configuración del puerto del menú principal, después elija un **puerto**, la salida indica si el modo rápido del puerto está habilitado. Esta salida está para el FastEthernet 0/26 del puerto, que es el puerto "A" en este Switch.

Catalyst 1900 - Port A Configuration

Built-in 100Base-FX

802.1d STP State: Blocking Forward Transitions: 0

----- Settings -----

[D] Description/name of port	
[S] Status of port	Suspended-no-linkbeat
[I] Port priority (spanning tree)	128 (80 hex)
[C] Path cost (spanning tree)	10
[H] Port fast mode (spanning tree)	Enabled
[E] Enhanced congestion control	Disabled
[F] Full duplex / Flow control	Half duplex

----- Related Menus -----

[A] Port addressing	[V] View port statistics
[N] Next port	[G] Goto port
[P] Previous port	[X] Exit to Main Menu

Enter Selection:

Pruebas de sincronización en el Catalyst 1900

Es más difícil verificar los valores de temporización en un 1900/2820 por la falta de herramientas de depuración, por lo que iniciamos un ping desde una PC conectada al switch dirigida al mismo switch. Entonces desconectamos y volvimos a conectar el cable y registramos en cuánto tiempo tomó para que el Switch responda al ping con Portfast y con Portfast apagado. Para un acceso de Ethernet con Portfast encendido (el estado predeterminado), el PC recibió una respuesta en el plazo de **5-6 segundos**. Con Portfast apagado la PC recibió una respuesta en 34 a 35 segundos.

Beneficio adicional de Portfast

Hay otro que atraviesa - árbol - la ventaja relacionada al uso de Portfast en su red. Un link se convierte en active y se mueve cada vez al estado de reenvío en atravesar - el árbol, el Switch envía un paquete del árbol de expansión especial llamado un Topology Change Notification (TCN). La notificación TCN se pasa hasta la raíz de atravesar - el árbol, donde se propaga a todo el Switches en el VLA N. Esto hace todo el Switches envejecer hacia fuera su tabla de direcciones MAC con el parámetro de retardo de reenvío. El parámetro de retardo de reenvío normalmente está configurado en 15 segundos. Cada vez que un puesto de trabajo se une a al Grupo de Bridge, las direcciones MAC en todo el Switches se envejecen hacia fuera después de 15 segundos en vez de los 300 segundos normales.

Dado que cuando una estación de trabajo entra en actividad, en realidad no cambia la topología en ninguna medida importante, en lo que respecta a todos los switches en la VLAN, no es necesario que atraviesen el período TCN de rápido vencimiento. Si usted gira el portfast, el Switch no envía los paquetes TCN cuando un puerto llega a ser activo.

Los comandos de utilizar para verificar la configuración trabajan

Ésta es una lista de comandos de utilizar cuando usted verifica si la configuración trabaje.

4000/5000/6000

- show port spantree 2/1; vea si la característica "Fast-Start" (Portfast) está activada o desactivada
- show spantree 1 - Controlar todos los puertos en VLAN 1 y verificar que tengan activado "Fast-Start" (Inicio rápido)
- show port channel – vea si tiene algunos canales activos
- show port channel 2 – consulte el modo de canal (automático, desconectado, etcétera) para cada puerto en el módulo 2
- show trunk 2 – consulte el modo de troncal (automático, desconectado, etcétera) para cada puerto en el módulo 2
- show port - muestra el estado (conectado, no conectado, etcétera), la velocidad, el dúplex para todos los puertos en el switch

2900XL/3500XL

- show spanning-tree interface FastEthernet 0/1 – para ver si Portfast está habilitado en este puerto (si Portfast no se menciona es que no está habilitado)
- show running-config - si un puerto muestra el comando spanning-tree portfast, la función

Portfast está habilitada.

1900/2800

- show running-config - para ver las configuraciones actuales (algunos comandos son invisibles cuando representan los valores predeterminados de la configuración del switch)
- Utilice el sistema de menús a la pantalla de estado del puerto

Comandos de utilizar para resolver problemas la configuración

Ésta es una lista de comandos de utilizar para resolver problemas la configuración.

4000/5000/6000

- show port spantree 2/1; vea si la característica "Fast-Start" (Portfast) está activada o desactivada
- show spantree 1 - Controlar todos los puertos en VLAN 1 y verificar que tengan activado "Fast-Start" (Inicio rápido)
- show port channel – vea si tiene algunos canales activos
- show port channel 2 – consulte el modo de canal (automático, desconectado, etcétera) para cada puerto en el módulo 2
- show trunk 2 – consulte el modo de troncal (automático, desconectado, etcétera) para cada puerto en el módulo 2
- show port - muestra el estado (conectado, no conectado, etc.), la velocidad, el dúplex para todos los puertos en el switch
- **registro de la demostración** - vea qué tipo de mensaje genera la salida de registro
- **fije el spantree 7 del nivel de registro** - fija el Switch para registrar el puerto de árbol de expansión, estado el tiempo real en la consola
- set port disable 2/1 – Desactive el puerto en software (como "apagado" en el router)
- set port enable 2/1 - activa el puerto en el software (como "no shutdown" en el router)
- **el tiempo de la demostración** - muestre la hora actual en los segundos (usados al inicio de una prueba de temporización)
- show port capabilities – vea que características se implementan en el puerto.
- set trunk 2/1 off - establecer el modo de conexión troncal en off (para acelerar el tiempo de inicialización del puerto)
- set port channel 2/1-2 off - establecer el modo EtherChannel (PAgP) en off (para acelerar el tiempo de inicialización del puerto)
- **set port speed 2/1 100** - fije el puerto a 100Mbps y apague la negociación automática
- set port duplex 2/1 full: Establece el dúplex de puerto completo

2900XL/3500XL

- service timestamps debug uptime - muestra la hora con los mensajes de depuración
- service timestamps log uptime - muestra la hora con los mensajes del registro.
- **debug spantree events** - muestre cuando el puerto se mueve con atravesar - etapas del árbol
- show clock - para ver el tiempo actual (para las pruebas de sincronización)
- show spanning-tree interface FastEthernet 0/1 – para ver si Portfast está habilitado en este puerto (si Portfast no se menciona es que no está habilitado)
- **cerrado** - para apagar un puerto del software
- no shut (no cierre) - para activar un puerto desde el software.

- show running-config - para ver las configuraciones actuales (algunos comandos son invisibles cuando representan los valores predeterminados de la configuración del switch)

Multi-Layer Switching (MLS) IP de la configuración y del Troubleshooting

Objetivos

Este documento delinea el Troubleshooting básico del Multilayer Switching (MLS) para el IP. Esta característica se ha convertido en un método muy conveniente con el cual acelerar el funcionamiento de la encaminamiento con el uso de los circuitos integrados específicos a la aplicación dedicados (Asics). El ruteo tradicional se hace a través de una CPU central y de un software; El MLS descarga una porción significativa de encaminamiento (reescritura de paquetes) al hardware y también se ha llamado transferencia. MLS y conmutación de tres capas son términos equivalentes. El NetFlow feature del IOS es distinto, y no cubierto en este documento. El MLS también incluye el soporte para IPX (IPX MLS) y el (MPLS) de la multidistribución, pero este documento concentra exclusivamente en el Troubleshooting de IP básico MLS.

Introducción

A medida que se formulan mayores demandas a las redes, mayor será la necesidad de mejor rendimiento. Los PC están conectados cada vez más con los LAN, los WAN y Internet, y sus usuarios requieren el acceso rápido a las bases de datos, a los archivos/a las páginas web, a las aplicaciones conectadas en red, a otros PC, y al vídeo de flujo continuo. Para mantener las conexiones rápidas y confiables, las redes deben poder ajustar rápidamente a los cambios y a los errores y encontrar el mejor trayecto, todos mientras que siguen siendo tan invisibles como sea posible a los usuarios finales. Los usuarios finales que experimentan un flujo de información rápido entre sus PC y el servidor con lentitud de red mínima son los más felices. La determinación del mejor trayecto es la función primaria de los Routing Protocol, y ésta puede ser a proceso que exige a la CPU; un incremento del rendimiento significativo es ganado descargando una porción de esta función al hardware de Switching. Ésta es la punta de la característica MLS.

Hay tres componentes importantes de MLS: dos de ellos son el MLS-RP y el MLS-SE. El MLS-RP es el router con MLS habilitado, que realiza la función tradicional de la encaminamiento entre las subredes/los VLA N. El MLS-SE es un switch habilitado para MLS que, generalmente, requiere un router para el ruteo entre subredes/VLAN, aunque con hardware y software especial puede encargarse de la reescritura del paquete. Cuando un paquete atraviesa una interfaz enrutada, las porciones sin datos del paquete se modifican (reescriben) mientras el paquete se transfiere a su destino, salto a salto. La confusión puede presentarse aquí, puesto que parece que un dispositivo de la capa-dos está adquiriendo una tarea del capa tres; realmente, el Switch está reescribiendo solamente la información del capa tres, y "está conmutando" entre las subredes/los VLA N--el router es todavía responsable de los cálculos basados en estándares de la ruta y de la determinación del mejor trayecto. Mucha de esta confusión puede ser evitada si usted mentalmente mantiene las funciones de ruteo y Switching separadas, especialmente cuando, al igual que comúnmente el caso, se contienen dentro del mismo chasis (que con un MLS-RP interno). Piense en el MLS como una forma mucho más avanzada de ruta que oculta, con el caché guardado a parte del router en un Switch. Tanto el MLS-RP como el MLS-SE, junto con los requisitos mínimos correspondientes de hardware y software, se requieren para MLS.

El MLS-RP puede ser interno (instalado en un chasis del switch) o externo (conectado a través de un cable con un puerto troncal en el Switch). Los ejemplos de los MLS-RP internos son el (RSM) y el Route Switch Feature Card (RSFC) del módulo route-switch, que están instaladas en un slot o un supervisor de un miembro de Catalyst 5xxx Family, respectivamente; lo mismo aplica a la Multilayer Switch Feature Card el (MSFC) para el Catalyst 6xxx Family. Los ejemplos de MSL-RP externos incluyen cualquier miembro de los routers de las series Cisco 7500, 7200, 4700, 4500 o 3600. Para soportar generalmente la característica IP MLS, todos los MLS-RP requieren una versión de IOS mínima en los trenes 11.3WA o 12.0WA; consulte la documentación de la versión para los específicos. También, el **MLS se debe habilitar** para que un router sea un MLS-RP.

El MLS-SE es un switch con hardware especial. Para un miembro del Catalyst 5xxx Family, el MLS requiere que el supervisor haga un Netflow Feature Card (NFFC) instalar; el Supervisor IIG y el IIIG tienen uno por abandono. Además, se requiere como mínimo el software Catalyst OS 4.1.1. Observe que el tren 4.x tiene el “general deployment (GD) ido,” o los criterios del usuario final y blancos rigurosos pasajeros de la experiencia de campo para la estabilidad, así que marque el sitio Web de Cisco para las últimas versiones. IP MLS se admite y habilita automáticamente el para software y hardware Catalyst 6xxx con MSFC/PFC (otros routers tienen el MLS desactivado en forma predeterminada) Observe que el IPX MLS y MLS para multicasting puede tener diversos requisitos del hardware y software (IOS y el Catalyst OS). Más plataformas de Cisco admiten o admitirán la característica MLS. También, el **MLS se debe habilitar** para que un Switch sea un MLS-SE.

El tercer componente importante de MLS es el Protocolo de conmutación de capas múltiples (MLSP). Debido a que la comprensión básica de MLSP llega al fondo de MLS, y es esencial realizar la resolución de problemas de MLS eficazmente, describiremos aquí MLSP en detalle. El MLSP es utilizado por el MLS-RP y el MLS-SE para comunicar el uno con el otro; las tareas incluyen habilitar el MLS; instalando, poniendo al día o borrando los flujos (información de la memoria caché); y administrar y exportar estadísticas de flujo (la Exportación de datos de Netflow se describe en otra documentación). MLSP también le permite a MLS-SE conocer las direcciones de Control de acceso de medios (MAC, capa 2) de las interfaces habilitadas para MLS, revisar la máscara de flujo del MLS-RP (explicado más adelante en este documento) y confirmar que el MLS-RP está operacional. El MLS-RP envía el Multicast “hola” paquetes cada 15 segundos con el MLSP; Si faltan tres de estos intervalos, entonces el MLS-SE reconoce que el MLS-RP falló o que se perdió la conectividad con éste.

El diagrama ilustra tres esencial que se deba completar (con el MLSP) para que un acceso directo sea creado: el candidato, enabler y pasos del almacenamiento en memoria inmediata. Las comprobaciones para MLS-SE una entrada de MLS ocultada; si la entrada de memoria caché de MLS y la información del paquete hacen juego (un golpe), la encabezado del paquete se reescribe localmente en el Switch (un acceso directo o puente del router) en vez de enviado encendido al router como sucede normalmente. Los paquetes que no hacen juego y se envían encendido al MLS-RP son paquetes candidato; es decir, hay una posibilidad de conmutarlos localmente. Después de que pase el paquete candidato a través de la máscara de flujo MLS (explicada en una sección más adelante) y reescriba la información contenida en la encabezado del paquete (la porción de datos no se toca), el router la envía hacia el salto siguiente a lo largo del trayecto de destino. El paquete se denomina ahora paquete facilitador. Si el paquete vuelve al mismo MLS-SE del cual se fue, un acceso directo MLS se crea y se coloca en caché MLS; la reescritura para ese paquete y todos los paquetes similares que siguen (llamó un flujo) ahora es hecha localmente por el hardware del Switch en vez por del software del router. El mismo MLS-SE debe ver tanto los paquetes candidatos como los activadores para un flujo particular, a fin de que se cree un acceso directo de MLS (es por esto que la topología de red es importante para MLS). Recuerde, la punta del MLS es permitir el trayecto de comunicación entre dos dispositivos en diversos VLA N, conectados apagado del mismo Switch, para desviar al router, y aumenta el

rendimiento de la red.

Por el uso del flowmask (esencialmente una lista de acceso) el administrador puede ajustar el grado de similaridad de estos paquetes, y ajusta el alcance de los flujos: dirección destino; direcciones de origen y destino; o información de destino, origen y capa cuatro. Observe que el primer paquete de un flujo pasa siempre a través del router; localmente se conmuta desde entonces. Cada flujo es unidireccional; la comunicación entre los PC, por ejemplo, requiere la configuración y el uso de dos accesos directos. El objetivo principal de MLSP es configurar, crear y mantener estos accesos directos.

Estos tres componentes (el MLS-RP, el MLS-SE y MLSP) liberan para arriba a los recursos del router vitales permitiendo que otros componentes de la red tomen en algunas de sus funciones. El dependiente sobre la topología y la configuración, MLS proporciona un simple y altamente un método eficaz de funcionamiento de red creciente en el LAN.

Resolución de problemas de la tecnología IP MLS

Un diagrama de flujo para el troubleshooting básico IP MLS es incluido y discutido. Se deriva de la mayoría de los tipos comunes de casos MLS-IP abiertos con el sitio web del Soporte técnico de Cisco y hechos frente por nuestros clientes y ingenieros de soporte técnico hasta el tiempo que este documento fue creado. El MLS es una característica de robustez, y usted no debe tener ningún problema con ella; si se presenta un problema, éste debe ayudarle a resolver los tipos de problemas MLS IP que usted puede ser que haga frente probablemente. Se hacen algunas suposiciones esenciales:

- Usted es familiar con los pasos de configuración básicos requeridos para habilitar IP MLS en el router y el Switches, y ha completado estos pasos: vea los recursos enumerados en el extremo de este documento para el material excelente.
- El Routing IP se habilita en el MLS-RP (está prendido por abandono): si el comando no ip routing aparece en la configuración global de un **funcionamiento de la demostración**, se ha apagado, y el IP MLS no funciona.
- La conectividad del IP existe entre el MLS-RP y el MLS-SE: **haga ping los IP Addresses** del router del Switch, y busque los signos de exclamación (llamados las "explosiones ") para visualizar a cambio.
- Las interfaces MLS-RP están en un estado del "up/up" en el router: ingrese show ip interface brief en el router para confirmarlo.

Advertencia: Siempre que usted realice los cambios de configuración a un router previsto para ser permanente, recuerde salvar esos cambios con un **copy running-config starting-config** (versiones acortadas de este **mem del comienzo** y del **wr del funcionamiento de copia del comando** incluye). Se pierde si las recargas de router o se reajusta cualquier modificación de configuración. El RS, el RSFC y el MSFC son Routers, no Switches. Por el contrario, los cambios que se realizaron en el indicador del switch de un miembro de la familia Catalyst 5xxx o 6xxx, se guardan automáticamente.

Esta sección resuelve problemas la tecnología MLS IP.

1. ¿Se cumplen los requisitos mínimos de software y hardware? Actualice el MLS-RP y SE para satisfacer los requisitos mínimos de software y hardware. Para el MLS-RP, no se necesita ningún hardware adicional. Aunque el MLS se pueda configurar en las interfaces NON-trunked, la conexión al MLS-SE está generalmente a través de las interfaces VLAN (como

con un RS) o de enlace del soporte (puede ser configurado para llevar la información sobre VLAN múltiple configurando el ISL o 802.1q). También, recuerde que, a partir del tiempo de la publicación, sólo los miembros del 7500, 7200, 4700, 4500, y las familias del 3600 Router soportan el MLS externamente. Actualmente, solamente estos routers externos y el Routers que caben en las familias del Catalyst 5xxx o 6xxx Switch (como el RS y el RSFC para el Catalyst 5xxx Family, y el MSFC para el Catalyst 6xxx Family) pueden ser MLS-RP. MSFC también requiere la Tarjeta de características de políticas (PFC), ambas instaladas en Catalyst 6xx Supervisor. IP MLS ahora es una función estándar en el software de ruteo 12.0 y versiones posteriores del IOS. El software IOS más bajo que IOS 12.0 requiere generalmente un tren especial; para tal soporte IP MLS, instale las últimas imágenes de IOS 11.3 que tienen las cartas "WA" en sus nombres de fichero. Para el MLS-SE, un Netflow Feature Card (NFFC) se requiere para un miembro del Catalyst 5xxx Family; este indicador luminoso LED amarillo de la placa muestra gravedad menor está instalado en el módulo de Supervisor del switch de Catalyst, e incluido como hardware estándar en más nuevos supervisores de las Catalyst 5xxx Series (es decir, desde 1999). No se admite NFFC en los Supervisor I o II y es una opción para los primeros Supervisor III. Además, se necesita un mínimo de 4.1.1 CatOS para IP MLS. Por el contrario, para la familia Catalyst 6xxx, el hardware requerido viene como equipo estándar y MLS IP ha sido admitida desde la primera versión de software de CatOS 5.1.1 (de hecho, MLS IP es un ingrediente esencial y predeterminado por su alto rendimiento). Con el lanzamiento de nuevas plataformas y software que admiten IP MLS, es importante consultar la documentación y las notas de la versión y, en general, instalar la última versión en la serie menor que cumpla con sus requisitos de características. Verifique siempre las notas de la versión y consulte en la oficina de ventas local de Cisco para obtener nuevos desarrollos de características y soporte MLS. Los comandos fundidos para marcar el hardware y software instalado son **versión de la demostración** en el router y **módulo show** en el Switch. **Note:** El Catalyst 6xxx Family del Switches no soporta un MLS-RP externo ahora. El MLS-RP debe ser un MSFC.

2. ¿Están los dispositivos de origen y de destino en diversos VLAN del mismo MLS-SE, compartiendo un solo campo común MLS-RP? Es un requisito básico de topología de MLS que el router tenga un trayecto hacia cada una de las VLAN. Recuerde que el objetivo de MLS es la creación de un atajo entre dos VLAN para que el switch pueda realizar el "ruteo" entre los dos dispositivos extremos, lo cual libera al router para que pueda realizar otras tareas. El Switch no rutea realmente; reescribe las tramas de modo que aparezca al final los dispositivos que hablan a través del router. Si los dos dispositivos están en el mismo VLAN, el MLS-SE conmuta la trama localmente sin el uso del MLS, como el Switches hace en tal transparente Bridged Environment, y no se crea ningún acceso directo MLS. Uno puede tener routers y switches múltiples en la red, e incluso switches múltiples a lo largo del trayecto del flujo, pero el trayecto entre los dos dispositivos finales para los que uno desea tener un acceso directo de MLS debe incluir una sola MLS-RP para dicho trayecto. En otras palabras, el flujo desde la fuente al destino debe cruzar un límite de VLAN en la misma MLS-RP y un par de paquetes candidato y activador debe ser visto por el mismo MLS-SE para que se cree el acceso directo de MLS. Si estos criterios no se cumplen, el paquete se rutea normalmente sin el uso del MLS. Refiera a los documentos sugeridos en el extremo de este documento para los diagramas y las discusiones con respecto a soportado y las Topologías de red no admitida.
3. ¿MLS-RP contiene una sentencia `mls rp ip` tanto en su configuración global como de interfaz? Si una no está presente, agregue instrucciones `mls rp ip` adecuadamente en el MLS-RP. Excepto para los routers cuyas IP MLS se habilitan automáticamente (como en los

Catalyst 6xxx MSFC), este es un paso de configuración requerido. En la mayoría de los MLS-RP (routers configurados para IP MLS), este enunciado debe aparecer tanto en la configuración global como en la configuración de la interfaz. **Note:** Cuando usted configura el MLS-RP, también recuerde poner el **comando mls rp management-interface** bajo una de sus interfaces IP MLS. Este paso obligatorio dice al MLS-RP del cual la interfaz él debe enviar los mensajes mlsp para comunicarse con el MLS-SE. Nuevamente, es necesario colocar este comando únicamente bajo una interfaz.

4. ¿Hay alguna característica configurada en MLS-RP que desactive automáticamente MLS en la interfaz? Hay varias opciones de configuración en el router que no son compatibles con el MLS. Éstas incluyen contabilidad de IP, encriptación, compresión, seguridad IP, Traducción de direcciones de red (NAT) y Velocidad de acceso comprometida (CAR). Para más información, refiera a los links con respecto a la configuración de MLS IP incluida en el extremo de este documento. Los paquetes que atraviesan una interfaz del router configurada con ninguna de estas características se deben enrutar normalmente; no se crea ningún acceso directo MLS. Para que el MLS trabaje, inhabilite estas características en la interfaz MLS-RP. Otra característica importante que afecta a MLS son las listas de acceso, las de entrada y salida. La discusión adicional de esta opción es incluida bajo el "flowmasks."
5. ¿El MLS-SE reconoce la dirección MLS-RP? Para que MLS funcione, el switch debe reconocer al router como un MLS-RP. Los MLS-RP internos (una vez más, el RSM o RSFC en un miembro de la familia Catalyst 5xxx y el MSFC en un miembro de la familia Catalyst 6xxx) son reconocidos automáticamente por el MLS-SE en el que están instalados. Para el externo MLS-RP, uno debe informar explícitamente al Switch el direccionamiento del router. Este direccionamiento no es realmente una dirección IP, aunque en el externo MLS-RP se elija de la lista de IP Addresses configurada en las interfaces del router; es simplemente una identificación del router de hecho, para los MLS-RP internos, el MLS-ID es normalmente ni siquiera una dirección IP configurada en el router; puesto que los MLS-RP internos se incluyen automáticamente, es comúnmente un Loopback Address (127.0.0.x). Para que MLS funcione, incluya en MLS-SE el MLS-ID que se encuentra en MLS-RP. Utilice los **mls rp de la demostración** en el router para encontrar el MLS-ID. Entonces configure ese ID en el Switch con el comando del **set mls include <MLS-ID>**. Esto es un paso de configuración necesario cuando usted utiliza el externo MLS-RP. **Note:** Si usted cambia la dirección IP del MLS-RP interconecta y entonces recargue al router, él puede hacer el proceso MLS en el router elegir un nuevo MLS-ID. Este nuevo MLS-ID puede ser diferente del MLS-ID que fue incluido manualmente en el MLS-SE, que puede hacer que el MLS pare; éste es una no falla del software, sino un efecto del Switch que intenta comunicarse con un MLS-ID que sea no más válido. Esté seguro de incluir este nuevo MLS-ID en el Switch para que el MLS trabaje de nuevo. Puede ser necesario inhabilitar/IP MLS del permiso, también. **Note:** Cuando el MLS-SE no está conectado directamente con el MLS-RP, como con esta topología, el direccionamiento que se debe incluir en el MLS-SE puede aparecer mientras que el Loopback Address mencionó: un switch conectado entre MLS-SE y MLS-RP. Debe incluir MLS-ID aunque MLS-RP sea interno. Al segundo Switch, el MLS-RP aparece como router externo puesto que el MLS-RP y el MLS-SE no se contienen en el mismo chasis.
6. ¿La interfaz de MLS-RP y el MLS-SE están en el mismo dominio VTP activado? El MLS requiere que los componentes MLS, incluyendo las estaciones terminales, deban estar en el mismo dominio del protocolo virtual trunking (VTP). El VTP es un protocolo de la capa-dos usado para manejar los VLAN en varios switches de Catalyst de un switch central. Permite a un administrador crear o borrar una VLAN en todos los switches en un dominio sin tener que hacerlo en cada switch en ese dominio. El Protocolo de conmutación multicapa (MLSP),

que utilizan el MLS-SE y MLS-RP para comunicarse, no cruza un límite del dominio VTP. Si el administrador de red tiene habilitado VTP en los switches (VTP está habilitado de forma predeterminada en los miembros de la familia Catalyst 5xxx y 6xxx), utilice el comando `show vtp domain` en el switch para detectar en qué dominio VTP se ha ubicado el MLS-SE. A excepción del Catalyst 6xxx MSFC, en el cual el MLS es esencialmente una *característica Plug and play*, usted debe agregar después el dominio VTP a cada uno de las interfaces MLS del router. Esto permite los Multicast MLSP se muevan entre el MLS-RP y el MLS-SE y permite que el MLS funcione. En el modo de configuración de la interfaz del MLS-RP, ingrese estos comandos: `no mls rp ip` Deshabilite la MLS en la interfaz MLS-RP afectada antes de modificar el dominio VTP. **el Domain Name del VTP-dominio <VTP rp de los mls > el Domain Name VTP** en cada interfaz habilitada para MLS deben hacer juego el del Switch. **VLAN-identificación rp de los mls <VLAN->** requerida solamente para conexión troncal no ISL, interfaces de MLS-RP externo. `mls rp management-interface` Ejecute este comando sólo en una interfaz en el RP MLS. Este paso necesario le indica al MLS-RP a qué interfaz debe enviar mensajes MLSP. **permiso MLS del IP rp de los mls** de nuevo en la interfaz del MLS-RP. Para cambiar el Domain Name VTP del MLS-SE, utilice este comando en el prompt del permiso de CatOS del Switch: `set vtp domain name <nombre de dominio VTP>` Para que MLS funcione, asegúrese de que VTP esté habilitado en el switch: `set vtp enable`

7. ¿Las máscaras de flujo coinciden sobre MLS-RP y MLS-SE? Una máscara de flujo es un filtro configurado por un administrador de red que es utilizado por MLS para determinar si se debe crear un acceso directo. Apenas como una lista de acceso, cuanto detallados los criterios que usted configura, el más profundo en el paquete el proceso MLS debe mirar para verificar si el paquete cumple esos criterios. Para ajustar el alcance de los accesos directos MLS-creados, el flowmask se puede hacer más o menos específico; el flowmask es esencialmente un dispositivo *que ajusta*. Hay tres tipos de modos MLS IP: destino ip, destination-source-ip, y full-flow-ip. El modo del destino ip, el valor por defecto, es funcionando cuando no se aplica ninguna lista de acceso a la interfaz habilitada para MLS del router. El modo del source-destination-ip es funcionando cuando una lista de acceso estándar es aplicada. La IP de flujo completo es de hecho para una lista de acceso ampliado. El modo MLS en el MLS-RP está implícitamente determinado por el tipo de lista de acceso aplicado a la interfaz. Por el contrario, el modo MLS del MLS-SE está explícitamente configurado. Si se elige el modo apropiado, el usuario puede configurar así el MLS de modo que solamente la dirección destino deba hacer juego para que un acceso directo MLS sea creado, o fuente y destino, o aún la información de la capa-cuatro como los números del puerto TCP/UDP. El modo MLS es configurable tanto con el MLS-RP como con el MLS-SE y, en general, deben coincidir. Si juzgan el source-destination-ip o a los modos MLS del full-flow-ip para ser requerido, es el mejor configurarlo en el router aplicando la lista de acceso apropiada. El MLS elige siempre la máscara más específica. Le da a la máscara de flujo configurada en el MLS-RP precedencia sobre la que se encuentra en el MLS-SE. **TENGA CUIDADO** si usted cambia al modo MLS del Switch del destino ip predeterminado: usted debe asegurarse que hace juego al modo MLS en el router para que el MLS trabaje. Para el source-destination-ip y los modos del full-flow-ip, recuerde aplicar la lista de acceso a la interfaz del router apropiada; sin la lista de acceso aplicada, incluso si está configurado, el modo MLS es simplemente destino ip, el valor por defecto. **Advertencia:** Siempre que se cambia la máscara de flujo, ya sea en MLS-RP o en MLS-SE, todos los flujos MLS almacenados en caché se borran y el proceso MLS se reinicia. Una purgación también puede ocurrir al aplicar el comando `clear ip route-cache` en el router. Si usted aplica el comando global `router configuration` **ningún Routing IP**, que apaga el Routing IP y

esencialmente transforma al router en un Bridge transparente, causa una purgación y una neutralización MLS (recuerde, ruteando es un requisito previo del MLS). Cada uno de éstos puede temporalmente, pero seriamente, rendimiento del router de la influencia en una red de producción. El router experimenta un punto en su carga hasta que se creen los nuevos accesos directos porque debe ahora manejar todos los flujos que fueron procesados previamente por el Switch. **Note:** Especialmente con un miembro del Catalyst 5000 Family como el MLS-SE, usted debe evitar el uso muy amplio del flowmasks que se configura con la información de la capa-cuatro. Si fuerzan al router a mirar tan profundamente en cada paquete en la interfaz, mucha de las ventajas previstas del MLS se desvía. Éste es mucho menos de un problema cuando usted utiliza a un miembro de Catalyst 6xxx Family como el MLS-SE puesto que los puertos del switch ellos mismos pueden reconocer la información de la capa-cuatro. **Note:** Hasta hace poco tiempo, el MLS no soportó entrante configurado flowmasks en una interfaz MLS-RP, solamente saliente. Si usted utiliza el **comando mls rp ip input-acl** además de los comandos configuration normales MLS-RP en una interfaz del router, se soporta un flowmask entrante.

8. ¿Son más que un par de MLS *demasiados* mensajes de error de los *movimientos* vistos continuamente en el Switch? Como la nota menciona, para cambiar un flowmask, borre memoria caché de ruta, o global dé vuelta apagado al Routing IP causa una purgación del caché. Otras circunstancias pueden también causar por completo o muchas purgaciones de la sola entrada y hacer el MLS quejarse de *demasiados movimientos*. Existen muchas formas de este mensaje, pero cada una contiene estas tres palabras: Independientemente de qué se ha mencionado ya, la mayoría de la causa común de este error es cuando el Switch aprende el Media Access Control (MAC) Address de Ethernet múltiples idénticas dentro del mismo VLA N; Las normas de Ethernet no permiten direcciones MAC idénticas dentro de la misma VLAN. Si está visto infrecuentemente, o apenas algunas veces en fila, no hay tema de inquietud; El MLS es una característica de robustez, y el mensaje se puede causar simplemente por los eventos de la red normal, como una conexión de PC que es movida entre los puertos, por ejemplo. Si está visto continuamente por varios minutos, es probable un síntoma de un más problema grave. Cuando se presenta tal situación, su causa raíz es comúnmente debido a la presencia de dos dispositivos con la misma dirección MAC conectada realmente con un VLA N, o a un loop físico dentro del VLA N (o de los VLAN múltiples si interliga a través de estos dominios de broadcast). Utilice el Troubleshooting del árbol de expansión (cubierto en otros documentos) y la extremidad para encontrar el loop y para eliminarlo. Además, cualquier cambio rápido en la topología puede causar inestabilidad temporaria en la red (y en MLS) como, por ejemplo, interfaces de router inestables, una mala tarjeta de interfaz de red (NIC), etc. **Consejo:** Utilice los **comandos show mls notification and show looktable** en el Switch de señalarle en dirección del MAC Address duplicado o del loop físico. El primer proporciona un valor TA. **El value>** del comando show looktable <TA vuelve una dirección MAC posible que se pueda localizar a la raíz del problema.

[Comandos o capturas de pantalla](#)

Para las descripciones y los ejemplos detallados del router MLS y de los comandos switch IP, refiera a la documentación enumerada bajo la [información relacionada](#)